Department of Homeland Security
Information Analysis and Infrastructure Protection Directorate

CyberNotes

Issue #2003-07 *April 7, 2003*

CyberNotes is published every two weeks by the Department of Homeland Security/Information Analysis and Infrastructure Protection (IAIP) Directorate. Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, Room 5905, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between March 18 and April 4, 2003. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
3com[1]	Multiple	SuperStack II RAS 1500	Two vulnerabilities exist: a remote Denial of Service vulnerability exists when network packets that contain malicious IP headers are processed; and a vulnerability exists due to inadequate authentication for various file requests, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	SuperStack II RAS 1500 Malicious IP Header Denial of Service & Inadequate Authentication	Low/ Medium (Medium if sensitive information can be obtained)	Bug discussed in newsgroups and websites. Exploit script has been published.

[1] iSEC Security Research Security Notice, March 24, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Adobe Systems, Inc.[2]	Windows 95/98/NT 4.0/2000, XP, MacOS, Unix	Acrobat 4.0 5, 4.0 5c, 4.0, 4.0.5 a, 5.0, 5.0.5, Acrobat Reader 4.0 5, 4.0 5c, 4.0, 4.0.5 a, 5.0, 5.0.5	A vulnerability exists in the implementation of the certification mechanism due to a failure to check the validity of a plug-in, which could let a malicious user produce false digital signatures to enable execution of arbitrary code.	No workaround or patch available at time of publishing.	Acrobat Plug-in Digital Signature CVE Name: CAN-2002-0030	**High**	Bug discussed in newsgroups and websites.
Alexan-dria/ Source Forge[3]	Windows, Unix	Alexandria Alexandria 2.0, 2.5; VA Software Source Forge Enterprise Edition 2.5, 2.7	Multiple vulnerabilities exist: a Cross-Site Scripting vulnerability exists due to insufficient filtering of HTML code, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists in the 'sendmessage.php' script due to insufficient validation of user-supplied data, which could let a remote malicious user send e-mail to arbitrary recipients; and a vulnerability exists in the 'docman/new.php' and 'patch/index.php' scripts due to insufficient checking, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing. Alexandria is no longer being actively maintained.	Alexandria/ Source Forge Multiple Vulnerabilities	Medium **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required.
Apache Software Founda-tion[4]	Unix	Apache 2.0.39-2.0.44	A vulnerability exists because file descriptors are improperly inherited by child processes, which could let a malicious user obtain sensitive information.	Upgrade available at: http://www.apache.org/dist/httpd/	Apache Web Server File Descriptor	Medium	Bug discussed in newsgroups and websites.
APC[5] ***More vendors release updates[6, 7, 8]***	**Unix**	**apcupsd 3.8.5**	**A vulnerability exists in the 'log_event' function due to a programming error, which could let remote malicious user obtain root access and possibly execute arbitrary code.**	**Upgrade available at:** **http://prdownloads.sourceforge.net/apcupsd/apcupsd-3.8.6.tar.gz?download** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** ***Debian:*** **http://security.debian.org/pool/updates/main/a/apcupsd/** ***SCO:*** **ftp://ftp.sco.com/pub/updates/OpenLinux/** ***SuSE:*** **ftp://ftp.suse.com/pub/suse**	**Apcupsd 'log_event' Remote Root Access** **CVE Name: CAN-2003-0098**	**High**	**Bug discussed in newsgroups and websites.**

[2] ElcomSoft Co. Ltd. Security Notice, March 24, 2003.
[3] Secunia Research, March 28, 2003.
[4] SecurityFocus, April 2, 2003.
[5] SecurityTracker Alert ID, 1006108, February 15, 2003.
[6] SCO Security Advisory, CSSA-2003-015.0, March 25, 2003.
[7] SuSE Security Announcement, SuSE-SA:2003:022, March 26, 2003.
[8] Debian Security Advisory, DSA 277-1, April 3, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
APC[9, 10, 11]	Unix	apcupsd 3.8.2, 3.8.5, 3.8.6	Several buffer overflow vulnerabilities exist, which could let a remote malicious user obtain elevated privileges or execute arbitrary code with root privileges.	**APC:** http://prdownloads.sourceforge.net/apcupsd/apcupsd-3.10.5.tar.gz?download **SuSE:** ftp://ftp.suse.com/pub/suse/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **SCO:** ftp://ftp.sco.com/pub/updates/OpenLinux/ **Debian:** http://security.debian.org/pool/updates/main/a/apcupsd/	Apcupsd Multiple Buffer Overflow CVE Name: CAN-2003-0099	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Apple[12]	Unix	MacOS X 10.2.4	A vulnerability exists in the Keychain Access application, which could let a malicious user obtain the Mac password.	**Workaround:** If using the Keychain Access application, ensure that all keychains are locked.	Apple Mac OS X Keychain Access Password Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required. Vulnerability has appeared in the press and other public media.
Apple[13]	Windows 95/98/ME/ NT 4.0/2000, MacOS 9.x, MacOS X 10.x	QuickTime Player 5.0.2 , 6	A buffer overflow vulnerability exists due to a failure to handle long URLs, which could let a remote malicious user execute arbitrary commands.	Upgrade available at: http://www.apple.com/quicktime/download/	QuickTime Long URL Buffer Overflow CVE Name: CAN-2003-0168	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[9] SCO Security Advisory, CSSA-2003-015.0, March 25, 2003.
[10] SuSE Security Announcement, SuSE-SA:2003:022, March 26, 2003.
[11] Debian Security Advisory, DSA-277, April 3, 2003.
[12] SecurityTracker Alert ID, 1006336, March 20, 2003.
[13] iDEFENSE Security Advisory 03.31.03, March 31, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Axis Communications[14] ***Axis issues workaround***[15]	**Multiple**	**2100 Network Camera 2.00- 2.03, 2.12, 2.30-2.33, 2130 PTZ Network Camera 2.32, 2400 Video Server 1.01, 1.02, 1.10-1.12, 1.15, 2.20, 2.31-2.33**	**Several vulnerabilities exist: a vulnerability exists because sensitive information is not properly secured, which could let a malicious user obtain sensitive information; and a vulnerability exists in the 'command.cgi' script because input is not properly handled, which could let a malicious user cause a Denial of Service and potentially execute arbitrary code.**	***Workaround available at:*** **http://www.securityfocus.com/archive/1/316184**	**Axis Communications Multiple Vulnerabilities**	**Low/ Medium/ High** **(Low if a Denial of Service; Medium is sensitive information can be obtained; and High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.**
BEA Systems[16]	Windows NT 4.0/2000, Unix	WebLogic Express 7.0.0.1, 7.0.0.1 SP1&2, 7.0, 7.0 SP1&2, WebLogic Express for Win32 7.0, 7.0 SP1, 7.0.0.1, 7.0.0.1 SP1, Weblogic Server 7.0, 7.0 SP1&2, 7.0.0.1, 7.0.0.1 SP1&2, WebLogic Server for Win32 7.0, 7.0 SP1, 7.0.0.1, 7.0.0.1 SP1	A vulnerability exists because the hostname is revealed, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	WebLogic Remote Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[14] 2002@WebSec.org Security Report, February 28, 2003.
[15] Axis Product Security, March 25, 2003.
[16] Bugtraq, April 2, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Beanwebb[17]	Unix	Guestbook 1.0	Several vulnerabilities exist: a vulnerability exists in the 'add.php' script due to inadequate HTML filtering, which could let a remote malicious user execute arbitrary code; and a vulnerability exists in the 'admin.php' script due to insufficient permissions, which could let a remote malicious user obtain unauthorized administrative access.	No workaround or patch available at time of publishing.	Guestbook 'add.php' & 'admin.php'	**High**	Bug discussed in newsgroups and websites. There is no exploit code required for the 'add.php' vulnerability. Proof of Concept exploit has been published for the 'admin.php' vulnerability.
Bernd Moon[18]	Windows Unix	Planet Moon Guestbook	A vulnerability exists in the 'Guestbook tr3.a' software password file, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Planetmoon Guestbook Password Retrieval	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
CGI City[19]	Unix	CCLog	A vulnerability exists in the 'cc_log.pl' script due to insufficient filtering of HTTP headers, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.icthus.net/CGI-City/scr_cgicity.shtml#CCLOG	CCLog HTTP Header HTML Injection	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
CGI-City[20]	Unix	CCGuest Book	A vulnerability exists in the 'cc_guestbook.pl' script due to insufficient HTML filtering, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.icthus.net/CGI-City/scr_cgicity.shtml#CCGUEST	CCGuestBook HTML Injection	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Check Point Software[21]	Windows NT 4.0, 2000, Unix	Next Generation FP3, FP3 HF1&HF2	Two vulnerabilities exist: a remote Denial of Service vulnerability exists in the syslog daemon; and vulnerability exists because escape characters are not properly filtered, which could let a remote malicious user execute arbitrary commands.	Hotfix available at: http://www.checkpoint.com/techsupport/ng/fp3_hotfix.html	Check Point VPN-1/ Firewall-1 Remote Syslog Vulnerabilities	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Chi Kien Uong[22]	Multiple	Advanced Poll 2.02	An information disclosure vulnerability exists, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Advanced Poll Remote Information Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

[17] Bugtraq, March 29, 2003.
[18] Bugtraq, March 21, 2003.
[19] Bugtraq, March 29, 2003.
[20] Bugtraq, March 29, 2003.
[21] Securiteam, March 23, 2003.
[22] SecurityFocus, March 22, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Clear swift Limited[23] ***Permanent fix available*** [24]	**Windows NT 4.0/2000**	**Mail Sweeper 4.0**	**A vulnerability exists because certain malformed MIME e-mail message attachments are not properly processed, which could let a remote malicious user bypass mail attachment filtering mechanisms.**	***Permanent fix available at:*** **http://www.clearswift.com/download/SQL/downloadList.asp?productID=301**	**MailSweeper Attachment Filter Bypass** **CVE Name: CAN-2003-0121**	**Medium**	**Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.**
Control Break International[25]	Windows	SafeBoot 3.5, 4.0, 4.0 SP1-SP2a, 4.1, SP1&SP2	An information disclosure vulnerability exists in the encryption software because an authentication failure error message is returned that indicates if the username or password is incorrect, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	SafeBoot Error Message Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Cooolsoft [26]	Windows NT 4.0/2000	PowerFTP 2.25	A buffer overflow vulnerability exists when overly long values are supplied for some FTP commands, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	No workaround or patch available at time of publishing.	PowerFTP FTP Command Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
D-Link Systems, Inc.[27]	Multiple	DSL-300 1.14, DSL-300G 2.00, DSL-500 1.14	Multiple vulnerabilities exist: a vulnerability exists because predictable default SNMP community strings are used, which could let a remote malicious user obtain sensitive information; and a vulnerability because passwords are stored in plaintext, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	DSL Router SNMP Default Community String & Plaintext Password	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited with a SNMP client. There is no exploit code required. for the password storage vulnerability
D-Link Systems, Inc.[28]	Multiple	DI-614+ 2.0	A remote Denial of Service vulnerability exists in the Internet Protocol (IP) due to the way fragmented IP packets are reassembled.	No workaround or patch available at time of publishing.	DI-614+ IP Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
DS Ltd. [29]	Unix	ViewPoint Server	A vulnerability exists because the /tmp directory is passed to the browser in cleartext, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	ViewPoint Server Information Disclosure	Medium	Bug discussed in newsgroups and websites.

[23] Corsaire Security Advisory, March 7, 2003.
[24] Bugtraq, March 26, 2003.
[25] IRM Security Advisory No. 003, March 20, 2003.
[26] Security Corporation Security Advisory, SCSA-015, April 1, 2003.
[27] Arhont Ltd Information Security Company Advisory, March 27, 2003.
[28] Bugtraq, March 26, 2003.
[29] Bugtraq, April 1, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
eDonkey & Overnet[30]	Multiple	eDonkey 2000 Client 0.44, 0.45; Overnet Overnet 0.44	A Denial of Service vulnerability exists when numerous chart dialog boxes are opened.	Upgrade available at: http://64.246.30.71/files/eDonkey0.46.exe	eDonkey Clients Multiple Chat Dialog Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Elad Rosenberg[31]	Windows	MyGuest BK	Two vulnerabilities exist: a Cross-Site Scripting vulnerability exists in the 'Add Entry' page due to insufficient filtering of user-supplied URI parameters, which could let a remote malicious user execute arbitrary HTML and script code; and a vulnerability exists in the administration panel because administrative functions can be accessed without prior authorization, which could let a malicious user obtain unauthorized administrative access.	No workaround or patch available at time of publishing.	MyGuestBK Add.asp Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Emule[32]	Windows	Emule 0.27b	A remote Denial of Service vulnerability exists when a malicious user submits a chat request without a nickname.	No workaround or patch available at time of publishing.	Emule Empty Nickname Chat Request Remote Denial Of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Ethereal Group[33, 34, 35, 36] ***SuSE releases advisory***[37]	**Unix**	**Ethereal 0.8.18**	**Two vulnerabilities exist: a format string vulnerability exists in the SOCKS dissector, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code; and a vulnerability exists in the NTLMSSP dissector, which could let a malicious user execute arbitrary code.**	**Upgrade available at:** **http://www.ethereal.com/distribution/ethereal-0.9.10.tar.gz** **Debian:** **http://security.debian.org/pool/updates/main/e/ethereal/** ***SuSE:*** **ftp://ftp.suse.com/pub/suse**	**Ethereal SOCKS Dissector Format String & NTLMSSP Overflow** **CVE Name: CAN-2003-0081**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites. Exploit scripts have been published.**
Francisco Burzi[38]	Windows, Unix	PHP-Nuke 6.5, 6.5 BETA 1, 6.5 RC1-RC3	A Cross-Site Scripting vulnerability exists in the 'block-Forums.php' script due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PHP-Nuke Block-Forums.PHP Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required.

[30] Bugtraq, March 21, 2003.
[31] Secunia Security Advisory, March 31, 2003.
[32] Bugtraq, March 25, 2003.
[33] Georgi Guninski Security Advisory #60, March 8, 2003.
[34] Ethereal Advisory, enpa-sa-00008, March 7, 2003.
[35] Debian Security Advisory, DSA 258-1, March 10, 2003.
[36] Gentoo Linux Security Announcement, 200303-10, March 9, 2003.
[37] SuSE Security Announcement, SuSE-SA:2003:019, March 21, 2003.
[38] Bugtraq, March 31, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Francisco Burzi[39]	Windows, Unix	PHP-Nuke 5.6, 6.0, 6.5, 6.5 RC1-RC3	Two vulnerabilities exist: a vulnerability exists in the ‘article.php’ file, which could let a malicious user obtain unauthorized access; and a vulnerability exists in the ‘ndex.php’ file, which could let a malicious user manipulate the database and alter information on articles posted on the site.	No workaround or patch available at time of publishing.	PHPNuke ‘article.php’ & ‘index.php’	Medium	Bug discussed in newsgroups and websites. Exploit has been published
Francisco Burzi[40]	Windows, Unix	PHP-Nuke 5.6, 6.0, 6.5, 6.5 RC1-RC3	A vulnerability exists in the ‘banners.php’ file, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	PHPNuke ‘Banners.php’ Password Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Francisco Burzi[41]	Windows, Unix	PHP-Nuke 6.5	A file disclosure vulnerability exists in the ‘viewpage.php’ script, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	PHPNuke Viewpage.PHP File Disclosure	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
global SCAPE, Inc. [42] ***Exploit script has been released***[43]	**Windows**	**CuteFTP 5.0**	**A buffer overflow vulnerability exists due to insufficient bounds checking on FTP command responses, which could let a malicious user execute arbitrary code.**	**No workaround or patch available at time of publishing.**	**CuteFTP Buffer Overflow**	**High**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.** ***Exploit script has been published.***
Gzip.org [44] ***More updates issued***[45, 46] ***NetBSD issues update***[47]	**Unix**	**zlib 1.1.4**	**A buffer overflow vulnerability exists in the compression library due to insufficient bounds checking of user-supplied data to the gzprintf() function, which could let a malicious user execute arbitrary instructions.**	**OpenPKG:** **http://www.openpkg.org/security/OpenPKG-SA-2003.015-zlib.html** ***SCO:*** **ftp://ftp.sco.com/pub/updates/OpenLinux** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php** ***NetBSD:*** **ftp://ftp.netbsd.org/pub/NetBSD/security/patches/**	**Zlib gzprintf() Buffer Overflow** **CVE Name: CAN-2003-0107**	**High**	**Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.**

[39] Bugtraq, March 22, 2003.
[40] SecurityFocus, March 21, 2003.
[41] Bugtraq, March 25, 2003.
[42] Bugtraq, January 18, 2003.
[43] SecurityFocus, March 29, 2003.
[44] OpenPKG Security Advisory, OpenPKG-SA-2003.015, March 4, 2003.
[45] SCO Security Advisory, CSSA-2003-011.0, March 10, 2003.
[46] Mandrake Linux Security Update Advisory, MDKSA-2003:033, March 18, 2003.
[47] NetBSD Security Advisory, 2003-004, March 26, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Company [48]	Multiple	MPE/iX 5.5, 6.5, 7.0, 7.5	A vulnerability exists in the FTP binary, which could let a remote malicious user obtain sensitive information.	Patches available at: http://itrc.hp.com/ Patch FTPGDY7, Patch FTPGDY8, Patch FTPGDY9	MPE/iX FTP Privileged Data Access	Medium	Bug discussed in newsgroups and websites.
Hewlett Packard Company [49]	Unix	HP-UX 11.0	A buffer overflow vulnerability exists in the IPCS interprocess communication status utility due to insufficient bounds checking of core file names, which could let a malicious user execute arbitrary code.	Users should contact the vendor for details on obtaining possible patches.	HP-UX IPCS Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Hewlett Packard Company [50, 51]	Windows NT 4.0/2000	Instant TopTools 5.0 4	A remote Denial of Service exists in the 'hpnst.exe' application because some types of requests are not handled properly.	Upgrade available at: http://h20004.www2.hp.com/soar_rnotes/bsdmatrix/matrix50459en_US.html#Utility%20-%20HP%20Instant%20Toptools	Instant TopTools Remote Denial of Service CVE Name: CAN-2003-0169	Low	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

[48] Hewlett-Packard Company Security Bulletin, HPSBMP0303-016, April 1, 2003.

[49] SecurityTracker Alert ID, 1006392, March 27, 2003.

[50] Digital Defense Inc. Security Advisory, DDI-1012, March 31, 2003.

[51] Hewlett-Packard Company Security Bulletin, HPSBMI0303-003, March 31, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Company [52] *Advisory updated*[53]	Unix	Compaq Tru64 4.0g, 4.0g PK3 (BL17), 4.0f, 4.0f PK7 (BL18), PK6 (BL17), 5.0a, 5.0a PK3 (BL17), 5.1a, 5.1a PK3 (BL3), PK2 (BL2), PK1 (BL1), 5.1, 5.1 PK6 (BL20), PK5 (BL19), PK4 (BL18), PK3 (BL17); HP HP-UX 11I, 8.0-8.2, 8.4-8.9, 9.0, 9.1, 9.3-9.10, 10.01, 10.0, 10.1, 10.8-10.10, 10.16, 10.20 SIS, 10.20 Series 700 & 800, 10.20, 10.24, 10.26, 10.30, 10.34, 11.04, 11.0, 11.11, 11.20, 11.22	A vulnerability exists because I/O that are opened by a setuid process may be assigned file descriptors equivalent to those used by the C library as 'standard input', 'standard output', and 'standard error,' which could let an untrusted malicious user write data to sensitive I/O channels and possibly compromise root.	Patches available at: ftp://ftp1.support.compaq.com/public/unix/ *Update to an existing patch available at:* http://ftp.support.compaq.com/patches/public/unix/v4.0g/t64v40gb17-c0028500-17206-es-20030305.README	HP Tru64/ HP-UX C Library Standard I/O File Descriptor	Medium/ High (High if root can be compromised)	Bug discussed in newsgroups and websites.

[52] Hewlett-Packard Company Software Security Response Team Bulletin, SSRT0845U, March 18, 2003.
[53] Hewlett-Packard Company Software Security Response Team Bulletin, SSRT0845U, March 27, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hot-Things.net [54]	Windows, Unix	Simple Chat! 1.0-1.3	An information disclosure vulnerability exists because sensitive information is not restricted, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Simple Chat Information Disclosure	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
HTML-Helper [55]	Windows	EZ Server 1.0	A remote Denial of Service vulnerability exists when a specific command that contains excessively long strings is executed.	No workaround or patch available at time of publishing.	EZ Server Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
IBM[56]	Unix	Tivoli Firewall Security Toolbox 1.2	Several buffer overflow vulnerabilities exist: a vulnerability exists in the 'relay.sh' script due to insufficient bounds checking on received data, which could let a remote malicious user execute arbitrary code and obtain root privileges; and a vulnerability exists in the relay daemon due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://www-3.ibm.com/software/sysmgmt/products/support/IBMTivoliManagementFramework.html	Tivoli Firewall Security Toolbox Buffer Overflows	**High**	Bug discussed in newsgroups and websites.
Instant Servers Inc.[57]	Windows	MiniPortal SOHO 1.3.3	A remote Denial of Service vulnerability exists because anonymous users are insufficiently restricted.	No workaround or patch available at time of publishing.	MiniPortal SOHO Anonymous Users Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Invision Power Services[58] ***Patch now available*** [59]	**Unix**	**Invision Board 1.1.1**	**A vulnerability exists in the 'ipchat.php' script due to insufficient sanitization or user-supplied data in URI parameters, which could let a remote malicious user execute arbitrary commands.**	***Patch available at:*** **http://forums.invisionpower.com/index.php?s=f0107570fbbd444b17ce6553cc1dc4a3&act=Attach&type=post&id=417579**	**Invision Board Remote File Include**	**High**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.**

[54] Bugtraq, March 20, 2003.
[55] Security Corporation Security Advisory, SCSA-014, March 31, 2003.
[56] Bugtraq, March 20, 2003,.
[57] Bugtraq, March 31, 2003.
[58] Bugtraq, February 27, 2003.
[59] SecurityFocus, March 26, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
ISC[60] ***Debian releases patch***[61] ***OpenPKG releases patch***[62] ***RedHat issues patch***[63]	**Unix**	**DHCPD 3.0.1 1 rc1-rc10**	**A remote Denial of Service vulnerability exists in 'dhcrelay' when a malicious bootp packet is submitted.**	**Debian:** **http://security.debian.org/pool/updates/main/d/dhcp3/** ***OpenPKG:*** **http://www.openpkg.org/security/OpenPKG-SA-2003.012-dhcpd.html** ***RedHat:*** **ftp://updates.redhat.com/**	**DHCPD dhcrelay Extraneous Network Packets Remote Denial of Service** **CVE Name: CAN-2003-0039**	**Low**	**Bug discussed in newsgroups and websites. Exploit has been published.**
ISC[64]	Unix	BIND 4.9, 4.9.2, 4.9.3, 4.9.4	A buffer overflow vulnerability exists in the resolver code due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	Upgrade available at: ftp://ftp.isc.org/isc/bind/src/4.9.5/bind-4.9.5-P1.tar.gz	BIND Resolver Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
jID[65]	Windows, Unix	WFChat 1.0d	An information disclosure vulnerability exists because sensitive information is stored in two known text files, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	WFChat Information Disclosure	Medium	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
Joel Palmius[66]	Unix	Mod_ Survey 3.0.9-3.0.15 – pre5	A vulnerability exists because data that is supplied via ENV tags is insufficiently sanitized, which could let a malicious user execute arbitrary code. Note: This is only an issue with surveys that use ENV tags.	Upgrades available at: http://gathering.itm.mh.se/modsurvey/download.php	Mod_Survey ENV Tags	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.

[60] Bugtraq, January 15, 2003.
[61] Debian Security Advisory, DSA 245-1, January 28, 2003.
[62] OpenPKG Security Advisory, OpenPKG-SA-2003.012, February 19, 2003.
[63] Red Hat Security Advisory, RHSA-2003:034-01, March 31, 2003.
[64] SecurityFocus, March 28, 2003.
[65] Bugtraq, March 19, 2003.
[66] Bugtraq, March 28, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Justice Media[67]	Windows, Unix	Media Guestbook 1.3	Several vulnerabilities exist: a vulnerability exists in the 'jgb.php3' script due to insufficient HTML filtering, which could let a malicious user execute arbitrary code; and a path disclosure vulnerability exists in the 'cfooter.php3' script, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Guestbook 'jgb.php3' & 'cfooter.php3" Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required for the 'jgb.php3' vulnerability. Proof of Concept exploit has been published for the 'cfooter.php3' vulnerability.
Kerio Technol-ogies[68]	Windows 95/98/ME/ NT 4.0/2000, XP	WinRoute Firewall 5.0.1	A remote Denial of Service vulnerability exists in the administration interface when a malicious user submits a malformed HTTP GET request.	No workaround or patch available at time of publishing.	WinRoute Firewall Malformed HTTP GET Request Remote Denial of Service	Low/**High** **(High if DDoS best practices not in place)**	Bug discussed in newsgroups and websites. There is no exploit code required.
Lilikoi Software, Inc. [69]	Windows NT 4.0, MacOS 9.0, BeOS, Unix	Lilikoi Ceilidh 2.60, 2.70	A Cross-Site Scripting vulnerability exists in the 'testcgi.exe' script due to insufficient filtering of some HTML code, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	Ceilidh Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Michael Jennings [70] ***Mandrake issues upgrade[71]***	**Unix**	**Eterm 0.8.10, 0.9.1**	**A vulnerability exists because the screen dump feature may be abused to corrupt local files that are writeable by the terminal user, which could let a local/remote malicious user obtain elevated privileges.**	**Upgrade available at: http://www.eterm.org/download/** ***Mandrake:*** **http://www.mandrakesecure.net/en/advisories/**	**Eterm Screen Dump Escape Sequence** **CVE Name: CAN-2003-0021**	**Medium**	**Bug discussed in newsgroups and websites. There is no exploit code required.**

[67] Bugtraq, March 29, 2003.
[68] Positive Technologies Security Advisory, 2003-0307, March 31, 2003.
[69] Security Corporation Security Advisory, SCSA-013, March 27, 2003.
[70] Bugtraq, February 24, 2003.
[71] Mandrake Linux Security Update Advisory, MDKSA-2003:040, April 1, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[72] ***Microsoft issues bulletin***[73]	**Windows NT 4.0/2000, XP**	**Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Professional, 2000 SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3**	**A remote Denial of Service vulnerability exists in the Remote Procedure Call (RPC) Service when a specifically malformed packet is sent to TCP port 135.**	***Frequently asked questions regarding this vulnerability and the patch can be found at:*** **http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-010.asp**	**Windows 2000 RPC Service Remote Denial of Service** **CVE Name: CAN-2002-1561**	**Low**	**Bug discussed in newsgroups and websites. Proofs of Concept exploit scripts have been published.**
Microsoft[74]	Windows NT 4.0/2000, XP	Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Professional, SP1-SP3, 2000 Server, SP1-SP3, 2000 Terminal Services, SP1-SP3, NT Terminal Server 4.0, SP1-SP6a, XP 64-bit Edition, SP1, XP Home, SP1, XP Professional, SP1	A vulnerability exists because Remote Desktop Protocol (RDP) clients do not attempt to validate the public key of the server to which they are connecting, which could let a malicious user initiate a man-in-the-middle attack.	No workaround or patch available at time of publishing.	Windows Remote Desktop Protocol Server Key Verification	Medium	Bug discussed in newsgroups and websites.

[72] Immunity Inc. Advisory, October 18, 2002.
[73] Microsoft Security Bulletin, MS03-010, March 26, 2003.
[74] Bugtraq, April 2, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [75]	Windows	ActiveSync 3.5	A remote Denial of Service vulnerability exists due to improper handling of some requests to the 'wcescomm' process when a malformed "sync request" packet is submitted.	No workaround or patch available at time of publishing.	Microsoft ActiveSync Remote Denial Of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft [76] ***Proof of Concept exploit released***[77]	**Windows 2000**	**Windows 2000, ISS 5.0**	**A buffer overflow vulnerability exists in the Windows component used by Web-based Distributed Authoring and Versioning (WebDAV) due to insufficient bounds checking on data, which could let a remote malicious user execute arbitrary code.**	**Frequently asked questions regarding this vulnerability and the patch can be found at:** **http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-007.asp**	**Windows 2000 WebDAV Buffer Overflow** **CVE Name: CAN-2003-0109**	**High**	**Bug discussed in newsgroups and websites.** **Vulnerability has appeared in the press and other public media.** ***Proof of Concept exploit script has been published.***
MIT[78] ***Vendors issue updates***[79, 80]	**Unix**	**Kerberos 4 Protocol**	**Multiple cryptographic vulnerabilities exist: a vulnerability exists in the xdrmem_getbytes() function due to faulty length checks, which could let a malicious user cause a Denial of Service or obtain unauthorized access to sensitive information; a vulnerability exists which could let a malicious user impersonate any principal in a realm that could result in a root-level compromise of the Domain Controller root-level compromise; and a vulnerability exists in the krb4 implementation that allows fabrication of Kerberos 4 tickets for unauthorized client principals if triple-DES keys are used to key Kerberos 4 services.**	**Patch available for Kerberos 5 with the affected Kerberos 4 code at:** **http://web.mit.edu/kerberos/www/advisories/2003-004-krb4_patchkit.tar.gz** ***Note: This patch is not for the Kerberos 4 standalone code.*** ***RedHat:*** **ftp://updates.redhat.com** ***Mandrake:*** **http://www.mandrakesecure.net/en/advisories/**	**Multiple Cryptographic Weaknesses in Kerberos 4**	**Low/ Medium/ High** **(Low if a DoS, Medium is sensitive information can be obtained, and High if a root compromise)**	**Bug discussed in newsgroups and websites.** **Vulnerability has appeared in the press and other public media.**

[75] IRM Security Advisory No. 004, March 21, 2003.
[76] Microsoft Security Bulletin, MS03-007 V1.1, March 18, 2003.
[77] Bugtraq, March 25, 2003.
[78] MIT krb5 Security Advisory, MITKRB5-SA-2003-003, March 19, 2003.
[79] Red Hat Security Advisory, RHSA-2003:051-01, March 26, 2003.
[80] Mandrake Linux Security Update Advisory, MDKSA-2003:043, April 1, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
MIT[81] ***Vendors issue updates***[82, 83]	**Unix**	**Kerberos 5 1.2.1-1.2.4**	**Multiple vulnerabilities exist: a vulnerability exists in various 'printf' functions due to a failure to supply sufficient format specifiers when handling user-supplied data, which could let a malicious user execute arbitrary commands; and a vulnerability exists due to insufficient bounds checking and sanitization of user-supplied data, which could let a remote malicious user cause a Denial of Service.**	**Upgrade available at:** **http://web.mit.edu/kerberos/www/krb5-1.2/index.html** ***RedHat:*** **ftp://updates.redhat.com** ***Mandrake:*** **http://www.mandrakesecure.net/en/advisories/**	**Kerberos Key Distribution Center Vulnerabilities** **CVE Name: CAN-2002-0036, CAN-2003-0060**	**Low/ High** **(High if arbitrary code is executed)**	**Bug discussed in newsgroups and websites.**
MIT[84, 85, 86, 87, 88]	Unix	Kerberos 5 1.0, 1.0.6, 1.1, 1.1.1, 1.2-1.2.7, 1.3 -alpha1	Several vulnerabilities exist: a buffer overflow vulnerability exists in the principal names array, which could let a malicious user cause a Denial of Service and execution of arbitrary code depending upon the malloc implementation; and a buffer overflow vulnerability exists in the principal names array due to unexpected results when calculating static values with user-supplied values, which could let a malicious user execute arbitrary code.	**MIT:** http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2003-005-patch.txt **RedHat:** ftp://updates.redhat.com/ **Debian:** http://security.debian.org/pool/updates/main/k/krb5/ **Mandrake:** http://www.mandrakesecure.net/en/advisories/	Kerberos 5 Principal Name Buffer Overflows CVE Names: CAN-2003-0072, CAN-2003-0082	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Mozilla[89]	Unix	Bonsai 1.3	Multiple vulnerabilities exist: a vulnerability exists which could let a remote malicious user execute arbitrary commands; and a vulnerability exists in the 'Edit Parameters' page, which could let a remote malicious user obtain unauthorized access.	**Debian:** http://security.debian.org/pool/updates/main/b/bonsai/	Mozilla Bonsai Multiple Remote Vulnerabilities CVE Names: CAN-2003-0152, CAN-2003-0155	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required.

[81] MIT krb5 Security Advisory, MITKRB5-SA-2003-001, January 28, 2003.
[82] Red Hat Security Advisory, RHSA-2003:051-01, March 26, 2003.
[83] Mandrake Linux Security Update Advisory, MDKSA-2003:043, April 1, 2003.
[84] MIT krb5 Security Advisory, 2003-005, March 20, 2003.
[85] Debian Security Advisory, DSA 266-1, March 24, 2003.
[86] Red Hat Security Advisory, RHSA-2003:051-01, March 26, 2003.
[87] Mandrake Linux Security Update Advisory, MDKSA-2003:043, April 1, 2003.
[88] Red Hat Security Advisory, RHSA-2003:091-01, April 1, 2003.
[89] Debian Security Advisory, DSA 265-1, March 21, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mozilla[90] ***Debian releases upgrades***[91]	**Unix**	**Bonsai 1.3**	**Multiple vulnerabilities exist: several Cross-Site Scripting vulnerabilities exist due to a lack of stripping of tags from user input, which could let a malicious user execute arbitrary script code; and a path disclosure vulnerability exists when a malformed request is submitted, which could let a malicious user obtain sensitive information.**	***Debian:*** **http://security.debian.org/pool/updates/main/b/bonsai/**	**Bonsai Multiple Cross Site Scripting & Path Disclosure Vulnerabilities** **CVE Names: CAN-2003-0153, CAN-2003-0154**	**Medium/ High** **(High if arbitrary code is executed)**	**Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.**
Multiple Vendors[92]	Multiple	Mozilla Browser 1.2 Alpha, 1.2.1; Netscape Navigator 7.0 2; Opera Software Opera Web Browser 7.0 win32, 7.0 1win32-7.0 3win32	A Denial of Service vulnerability exists when certain malformed JavaScript enabled pages are executed.	No workaround or patch available at time of publishing.	Multiple Vendor Web Browser JavaScript Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Multiple Vendors[93]	Windows 2000, Unix	ISC BIND 9.1-9.1.3, 9.2.0-9.2.2; Microsoft Windows 2000 Advanced Server, SP1-SP3, 2000 Datacenter Server, SP1-SP3, 2000 Server, SP1-SP3	A Denial of Service vulnerability exists due to the way some types of DNS requests are handled.	No workaround or patch available at time of publishing.	Multiple Vendor DNS Denial Of Service	Low	Bug discussed in newsgroups and websites.

[90] Bugtraq, August 19, 2002.
[91] Debian Security Advisory, DSA 265-1, March 21, 2003.
[92] Bugtraq, March 28, 2003.
[93] CERT Vulnerability Note, VU#714121, March 28, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[94, 95] *More vendors release upgrades*[96, 97, 98]	Unix	Linux kernel 2.2.1-2.2.23	A Denial of Service vulnerability exists in the MMap() implementation.	Trustix: ftp://ftp.trustix.net/pub/Trustix/updates/ *Engarde:* http://ftp.engardelinux.org/pub/engarde/stable/updates/ *RedHat:* ftp://updates.redhat.com/ *Mandrake:* http://www.mandrakesecure.net/en/ftp.php	Linux Kernel Denial of Service CVE Name: CAN-2002-1380	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Multiple Vendors[99] *RedHat releases upgrades*[100] *More vendors release upgrades*[101, 102, 103]	Windows 2000, Unix	FreeBSD 4.2-4.7; Linux kernel 2.4.1-2.4.20; Microsoft Windows 2000 Advanced Server, SP1-SP2, 2000 Datacenter Server, SP1-SP2, 2000 Professional, SP1-SP2, 2000 Server, SP1-SP2, 2000 Terminal Services, SP1-SP2; NetBSD NetBSD 1.5- 1.5.3, 1.6	A vulnerability exists because multiple platform Ethernet Network Interface Card (NIC) device drivers incorrectly handle frame padding due to incorrect implementations of RFC requirements and poor programming practices, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing. *RedHat:* ftp://updates.redhat.com/ *Engarde:* http://ftp.engardelinux.org/pub/engarde/stable/updates/ *Mandrake:* http://www.mandrakesecure.net/en/ftp.php	Multiple Vendor Network Device Driver Frame Padding Information Disclosure CVE Name: CAN-2003-0001	Medium	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[94] RAZOR Advisory, December 17, 2002.
[95] Trustix Secure Linux Security Advisory, 2002-0083, December 19, 2002.
[96] EnGarde Secure Linux Security Advisory, ESA-20030318-009, March 18, 2003.
[97] Red Hat Security Advisory, RHSA-2003:088-01, March 19, 2003.
[98] Mandrake Linux Security Update Advisory, MDKSA-2003:039, March 28, 2003.
[99] @stake, Inc. Security Advisory, A010603-1, January 7, 2003.
[100] Red Hat, Inc. Red Hat Security Advisory, RHSA-2003:025-20, February 4, 2003.
[101] EnGarde Secure Linux Security Advisory, ESA-20030318-009, March 18, 2003.
[102] Mandrake Linux Security Update Advisory, MDKSA-2003:039, March 27, 2003.
[103] Red Hat Security Advisory, RHSA-2003:088-01, March 19, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts

Multiple Vendors [104, 105, 106]	Unix	BSD lpr 2000.05.07, 0.48'
		FreeBSD FreeBSD 2.2-2.2.6;
		lpr-ppd lpr-ppd 0.72;
		lprold lprold 3.0.48;
		OpenBSD OpenBSD 2.0-2.9, 3.0-3.2
			A buffer overflow vulnerability exists in the 'lpr' printer spooling system, which could let a malicious user execute arbitrary code as root.	**Debian:**
				http://security.debian.org/pool/updates/main/l/lpr/
				SuSE:
				ftp://ftp.suse.com/pub/suse/
				OpenBSD:
				ftp://ftp.openbsd.org/pub/OpenBSD/patches/
					Multiple Vendor LPRM Buffer Overflow
					
					CVE Name: CAN-2003-0144
						High	Bug discussed in newsgroups and websites. Exploit scripts have been published.

Multiple Vendors [107]	Unix	Caldera UnixWare 7, 7.1.0, 7.1.1, 7.1.3;
		IBM AIX 4.0, 4.1-4.1.5, 4.2, 4.2.1, 4.3- 4.3.3, 5.1 L, 5.1, 5.2;
		SCO Open UNIX 8.0, UnixWare 7.0, 7.0.1, 7.1, 7.1.1, 7.1.3;
		Sun Solaris 2.5.1, 2.5.1_x86, 2.5.1_ppc, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, _x86, 9.0, _x86, 9.0_x86 Update 2,
		HP Tru64 UNIX 4.x, 5.x,
		HP-UX 10.x, 11.x
			A buffer overflow vulnerability exists in dtsession due to the way the HOME environment variable is handled, which could let a malicious user obtain root privileges.	**Sun:**
				http://sunsolve.Sun.COM/pub-cgi/retrieve.pl?doc=fsalert/52388
					Solaris dtsession HOME Buffer Overflow
					
					CVE Name: CAN-2003-0092
						High	Bug discussed in newsgroups and websites.

[104] SuSE Security Announcement, SuSE-SA:2003:0014, March 13, 2003.
[105] Debian Security Advisory, DSA 267-1, March 24, 2003.
[106] Debian Security Advisory, DSA 275-1, April 2, 2003.
[107] NSFOCUS Security Advisory, SA2003-03, March 31, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [108, 109, 110, 111] ***More vendors release upgrades*** [112, 113, 114, 115, 116]	**Unix**	**Linux kernel 2.2-2.2.24, 2.4-2.4.21 pre1**	**A vulnerability exists in the ptrace() system call due to a failure to restrict trace permissions on some root spawned processes, which could let a malicious user obtain root access.**	**Upgrade available at:** **ftp://ftp.kernel.org/pub/linux/kernel/v2.2/linux-2.2.25.tar.gz** **RedHat:** **ftp://updates.redhat.com/** **Engarde:** **ftp://ftp.engardelinux.org/pub/engarde/stable/updates/** **Trustix:** **http://www.trustix.net/pub/Trustix/updates/** ***Debian:*** **http://security.debian.org/pool/updates/main/k/** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php** ***SuSE:*** **ftp://ftp.suse.com/pub/suse**	**Linux Kernel Root Access** **CVE Name: CAN-2003-0127**	**High**	**Bug discussed in newsgroups and websites. Exploit scripts have been published.**

[108] Red Hat Security Advisory, RHSA-2003:098-00, March 17, 2003.
[109] EnGarde Secure Linux Security Advisory, ESA-20030318-009, March 18, 2003.
[110] Trustix Secure Linux Security Advisory, TSLSA-2003-0007, March 18, 2003.
[111] Red Hat Security Advisory, RHSA-2003:088-01, March 19, 2003.
[112] SuSE Security Announcement, SuSE-SA:2003:021, March 25, 2003.
[113] Debian Security Advisory, DSA 270-1, March 27, 2003.
[114] Mandrake Linux Security Update Advisory, MDKSA-2003:038, March 27, 2003.
[115] Mandrake Linux Security Update Advisory, MDKSA-2003:039, March 28, 2003.
[116] Debian Security Advisory, DSA 276-1, April 3, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [117, 118] *More vendors release upgrades* [119]	Unix	Cray UNICOS 6.0, 6.0 E, 6.1, 7.0, 8.0, 8.3, 9.0, 9.0.2.5, 9.2, 9.2.4; FreeBSD 4.0- 4.6, 4.7, 5.0, 4.1.1–4.7 Stable & Release; GNU glibc 2.1-2.1.3, 2.2-2.2.5, 2.3-2.3.2; HP HP-UX 10.20 Series 700 & 800, 10.20, 10.24, 11.04, 11.0, 11.11, 11.20, 11.22; IBM AIX 4.3.3, 5.1, 5.2; MIT Kerberos 5 1.2-1.2.7; OpenAFS 1.0-1.3.2; OpenBSD 2.0-3.2; SGI IRIX 6.5-6.5.20, 6.5m-6.5.20m, 6.5f-6.5.20f; Sun Solaris 2.5.1, 2.5.1_x86, 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86,, 9.0, 9.0_x86	An integer overflow vulnerability exists in the xdrmem_getbytes() function that is distributed as part of the Sun Microsystems XDR library, which could let a remote malicious user execute arbitrary code.	FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:05/xdr-4.patch SCO: ftp://ftp.sco.com/pub/updates/OpenLinux/ MIT: http://web.mit.edu/kerberos/www/advisories/2003-003-xdr_patch.txt RedHat: ftp://updates.redhat.com/ IBM: http://techsupport.services.ibm.com/r FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:05/xdr-4.patch *Debian:* http://security.debian.org/pool/updates/main/o/openssh-krb5/ *Mandrake:* http://www.mandrakesecure.net/en/ftp.php *NetBSD:* ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2003-008.txt.asc *Trustix:* http://www.trustix.net/pub/Trustix/updates/	Sun XDR Library xdrmem_getbytes() Integer Overflow CVE Name: CAN-2003-0028	High	Bug discussed in newsgroups and websites.

[117] eEye Security Advisory, AD20030318, March 19, 2003.
[118] CERT® Advisory, CA-2003-10, March 19, 2003.
[119] SecurityFocus, April 2, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [120], [121], [122], [123], [124], [125], [126], [127], [128], [129] ***Apple releases upgrade*** [130]	**Unix**	**FreeBSD 4.2-4.6, 4.6.2, 4.7, 4.7 Stable, 4.8 –PRE-RELEASE, 5.0; OpenBSD OpenBSD 3.1, 3.2; OpenSSL Project OpenSSL 0.9.1 c, 0.9.2 b, 0.9.3, 0.9.4, 0.9.5 a, 0.9.5, 0.9.6, 0.9.6 a-0.9.6 e, 0.9.6 g, 0.9.6 h, 0.9.7, 0.9.7 beta1-beta3**	**A vulnerability exists in implementations of SSL when CBC encryption is used because MAC computation is not performed if an incorrect block cipher padding is used, which could let a remote malicious user obtain sensitive information through analysis of the timing of certain operations.**	**FreeBSD:** **ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:02/** **OpenBSD:** **ftp://ftp.openbsd.org/pub/OpenBSD/patches/** **OpenSSL Project:** **http://www.openssl.org/source/openssl-0.9.6i.tar.gz** **SuSE:** **ftp.suse.com/pub/suse/i386/update/** **OpenPKG:** **ftp://ftp.openpkg.org/release** **Debian:** **http://security.debian.org/pool/updates/main/o/openssl/** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** **EnGarde:** **ftp://ftp.engardelinux.org/pub/engarde/stable/updates/** **Trustix:** **ftp://ftp.trustix.net/pub/Trustix/updates/** ***Apple:*** **http://docs.info.apple.com/article.html?artnum=61798**	**OpenSSL CBC Error Information Leakage** **CVE Name: CAN-2003-0078**	**Medium**	**Bug discussed in newsgroups and websites. Exploit has been published.**

[120] OpenPKG Security Advisory, OpenPKG-SA-2003.013, February 19, 2003.
[121] OpenSSL Security Advisory, February 19, 2003.
[122] Gentoo Linux Security Announcement, 200302-10, February 20, 2003.
[123] EnGarde Secure Linux Security Advisory, ESA-20030220-005, February 20, 2003.
[124] Mandrake Linux Security Update Advisory, MDKSA-2003:020, February 21, 2003.
[125] Trustix Secure Linux Security Advisory, TSLSA-2003-0005, February 21, 2003.
[126] Conectiva Linux Security Announcement, CLA-2003:570, February 24, 2003.
[127] Debian Security Advisory, DSA 253-1, February 24, 2003.
[128] FreeBSD Security Advisory, FreeBSD-SA-03:02, February 25, 2003.
[129] SuSE Security Announcement, SuSE-SA:2003:011, February 26, 2003.
[130] Apple Security Update, March 31, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [131, 132, 133, 134] ***More vendors release upgrades*** [135, 136, 137, 138, 139]	**Unix**	**OpenPKG Current, OpenPKG 1.1, 1.2; OpenSSL Project OpenSSL 0.9.6, 0.9.6a-0.9.6I, 0.9.7, 0.9.7a**	**A side-channel attack in the OpenSSL implementation has been published in a recent paper, which could let a remote malicious user obtain the RSA private key of a target server.**	**OpenPKG:** **ftp://ftp.openpkg.org/** **Trustix:** **ftp://ftp.trustix.net/pub/Trustix/updates/** **Engarde:** **ftp://ftp.engardelinux.org/pub/engarde/stable/updates/** **OpenBSD:** **ftp://ftp.openbsd.org/pub/OpenBSD/patches/3.1/common/024_blinding.patch** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php** ***NetBSD:*** **ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2003-007.txt.asc** ***FreeBSD:*** **ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:06/openssl.patch** ***RedHat:*** **ftp://updates.redhat.com/** ***SuSE:*** **ftp://ftp.suse.com/pub/suse**	**OpenSSL Timing Attack RSA Private Key Information Disclosure** **CVE Name: CAN-2003-0147**	**Medium**	**Bug discussed in newsgroups and websites. Exploit script has been published.**

[131] OpenPKG Security Advisory, OpenPKG-SA-2003.019, March 18, 2003.
[132] OpenPKG Security Advisory, OpenPKG-SA-2003.020, March 18, 2003.
[133] Trustix Secure Linux Security Advisory, TSLSA-2003-0010, March 18, 2003.
[134] EnGarde Secure Linux Security Advisory, ESA-20030320-010, March 20, 2003.
[135] Mandrake Linux Security Update Advisory, MDKSA-2003:035, March 25, 2003.
[136] NetBSD Security Advisory 2003-007, 2003-007, March 26, 2003.
[137] FreeBSD Security Advisory, FreeBSD-SA-03:06, March 26, 2003.
[138] Red Hat Security Advisory, RHSA-2003:101-01, April 1, 2003.
[139] SuSE Security Announcement, SuSE-SA:2003:024, April 4, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors [140, 141, 142, 143, 144, 145, 146, 147]	Unix	Sendmail Consortium Sendmail 8.9.0-8.9, 8.10-8.10.2, 8.11-8.11.6, 8.12 beta7, beta5, beta16, beta12, beta10, 8.12-8.12.8; Sendmail Inc. Sendmail for NT 2.6-2.6.2, 3.0- 3.0.3, Sendmail Switch 2.1-2.1.5, 2.2-2.2.5, 3.0-3.0.3; Sun Solaris 2.4, 2.4_x86, 2.5, 2.5_x86, 2.5.1, 2.5.1_x86, 2.5.1_ppc , 2.6, 2.6_x86, 7.0, 7.0_x86, 8.0, 8.0_x86, 9.0, 9.0_x86, 9.0_x86 Update 2; HP Tru64 UNIX 4.x, 5.x, HP-UX 10.x, 11.x	A buffer overflow vulnerability exists in the prescan() procedure due to the way long e-mail address are handled, which could let a remote malicious user execute arbitrary code with root privileges.	**Sendmail Consortium:** Upgrade available at: ftp://ftp.sendmail.org/pub/sendmail/sendmail.8.12.9.tar.gz Patch available at : ftp://ftp.sendmail.org/pub/sendmail/prescan.tar.gz.uu **RedHat:** ftp://updates.redhat.com/ **OpenBSD:** ftp://ftp.openbsd.org/pub/OpenBSD/patches/ **Slackware:** ftp://ftp.slackware.com/pub/slackware/slackware-8.0/patches/packages/sendmail.tgz **FreeBSD:** ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:07/ **Immunix:** http://download.immunix.org/ImmunixOS/7+/Updates/RPMS/ **OpenPKG:** ftp://ftp.openpkg.org/release/1.2/UPD/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **SuSE:** ftp://ftp.suse.com/pub/suse/ **Sun:** Linux Systems: http://sunsolve.sun.com/patches/linux/security.html Cobalt Legacy Products: ftp://ftp-eng.cobalt.com/pub/experimental/security/sendmail2 Sun advises affected users to discontinue using Sendmail (until a patch is available) by issuing the following command: /etc/init.d/sendmail stop	Sendmail Address Prescan Buffer Overflow CVE Name: CAN-2003-0161	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[140] CERT Advisory CA-2003-12, March 29, 2003.
[141] OpenPKG Security Advisory, OpenPKG-SA-2003.027, March 30, 2003.
[142] Slackware Advisory, 2003-03-31, March 31, 2003.
[143] Red Hat Security Advisory, RHSA-2003:120-01, March 31, 2003.
[144] FreeBSD Security Advisory, FreeBSD-SA-03:07, March 31, 2003.
[145] Immunix Secured OS Security Advisory, IMNX-2003-7+-002-01, April 1, 2003.
[146] Mandrake Linux Security Update Advisory, MDKSA-2003:042, April 1, 2003.
[147] SuSE Security Announcement, SuSE-SA:2003:023, April 1, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mutt[148, 149] ***More vendors release upgrades***[150, 151, 152, 153, 154]	**Unix**	**Mutt 1.3.16, 1.3.17, 1.3.22, 1.3.24, 1.3.25, 1.4.0, 1.5.3**	**A buffer overflow vulnerability exists because remote internationalized folders are not properly handled, which could let a malicious user execute arbitrary code.**	**Upgrade available at:** **ftp://ftp.mutt.org/mutt/mutt-1.4.1i.tar.gz** **OpenPKG:** **ftp://ftp.openpkg.org/release** ***Debian:*** **http://security.debian.org/pool/updates/main/m/mutt** ***Slackware:*** **ftp://ftp.slackware.com/pub/slackware/** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php** ***RedHat:*** **ftp://updates.redhat.com/** ***SuSE:*** **ftp://ftp.suse.com/pub/suse**	**Mutt Remote Folder Buffer Overflow** **CVE Name: CAN-2003-0140**	**High**	**Bug discussed in newsgroups and websites.**
Mutt[155, 156]	Unix	Mutt 1.3.12, 1.3.12-1, 1.3.16, 1.3.17, 1.3.22, 1.3.24, 1.3.25, 1.3.27, 1.3.28	A buffer overflow vulnerability exists due to insufficient verification of folder names, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	**Debian:** http://security.debian.org/pool/updates/main/m/mutt **SuSE:** ftp://ftp.suse.com/pub/suse/ **Slackware:** ftp://ftp.slackware.com/pub/slackware/ **Mandrake:**	Mutt IMAP Remote Folder Buffer Overflow CVE Name: CAN-2003-0167	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
MySQL AB[157, 158, 159] ***Engarde releases upgrade***[160]	**Unix**	**MySQL 3.23.52**	**A vulnerability exists in the 'mysqld' service, which could let a malicious user obtain elevated privileges as root.**	**Upgrade available at:** **http://www.mysql.com/downloads/mysql-3.23.html** **OpenPKG:** **ftp.openpkg.org** **Trustix:** **http://www.trustix.net/pub/Trustix/updates/** ***Engarde:*** **http://ftp.engardelinux.org/pub/engarde/stable/updates/**	**MySQL 'mysqld' Elevated Privileges** **CVE Name: CAN-2003-0150**	**High**	**Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.**

[148] Core Security Technologies Advisory, CORE-20030304-02, March 20, 2003.
[149] OpenPKG Security Advisory, OpenPKG-SA-2003.025, March 20, 2003.
[150] SuSE Security Announcement, SuSE-SA:2003:020, March 24, 2003.
[151] Debian Security Advisory, DSA 268-1, March 25, 2003.
[152] Slackware Security Advisory, 2003-03-30, March 30, 2003.
[153] Mandrake Linux Security Update Advisory, MDKSA-2003:041, April 1, 2003.
[154] Red Hat Security Advisory, RHSA-2003:109-03, April 3, 2003.
[155] SuSE Security Announcement, SuSE-SA:2003:020, March 24, 2003.
[156] Debian Security Advisory, DSA 268-1, March 25, 2003.
[157] OpenPKG Security Advisory, OpenPKG-SA-2003.022, March 18, 2003.
[158] Gentoo Linux Security Announcement, 200303-14, March 18, 2003.
[159] Trustix Secure Linux Security Advisory, 2003-0009, March 18, 2003.
[160] EnGarde Secure Linux Security Advisory, ESA-20030324-012, March 24, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
NetGear [161]	Multiple	FVS318 1.00, 1.1-1.3	A remote Denial of Service vulnerability exists because some types of input are not properly handled.	No workaround or patch available at time of publishing.	NetGear ProSafe VPN Firewall Web Remote Denial Of Service	Low/**High** **(High if DDoS best practices not in place)**	Bug discussed in newsgroups and websites. Exploit has been published.
Netpbm [162] ***More vendors release upgrades*** [163, 164]	**Unix**	**Netpbm 10.0-10.14**	**Multiple buffer overflow vulnerabilities exist due to math overflow errors, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.**	***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php** ***RedHat:*** **ftp://updates.redhat.com**	**Multiple Netpbm Remote Buffer Overflow** **CVE Name: CAN-2003-0146**	**Low/High** **(High if arbitrary code can be executed)**	**Bug discussed in newsgroups and websites.**
OpenSSL Project[165, 166, 167, 168, 169,]	Unix	OpenSSL 0.9.6i, 0.9.6h, 0.9.6g, 0.9.6e, 0.9.6d, 0.9.6c, 0.9.6b, 0.9.6a, 0.9.6, 0.9.7a, 0.9.7	A vulnerability exists because the response of vulnerable servers can be abused, which could let a remote malicious user obtain sensitive information.	**Mandrake:** http://www.mandrakesecure.net/en/ftp.php **OpenPKG:** ftp://ftp.openpkg.org/release **OpenBSD:** ftp://ftp.openbsd.org/pub/OpenBSD/patches/ **Engarde:** ftp://ftp.engardelinux.org/pub/engarde/stable/updates/ **NetBSD:** ftp://ftp.netbsd.org/pub/NetBSD/security/advisories/NetBSD-SA2003-007.txt.asc **FreeBSD:** ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-03:06/openssl.patch **OpenPKG:** http://www.openpkg.org/security.html	OpenSSL Side Channel Leakage CVE Name: CAN-2003-0131	Medium	Bug discussed in newsgroups and websites.

[161] SecurityTracker Alert ID, 1006337, March 20, 2003.
[162] Bugtraq, February 28, 2003.
[163] Mandrake Linux Security Update Advisory, MDKSA-2003:036, March 25, 2003.
[164] Red Hat Security Advisory, RHSA-2003:060-01, April 2, 2003.
[165] EnGarde Secure Linux Security Advisory, ESA-20030320-010, March 20, 2003.
[166] OpenPKG Security Advisory, OpenPKG-SA-2003.026, March 20, 2003.
[167] FreeBSD Security Advisory, FreeBSD-SA-03:06, March 21, 2003.
[168] Mandrake Linux Security Update Advisory, MDKSA-2003:035, March 25, 2003.
[169] NetBSD Security Advisory, 2003-007, March 26, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Opera Software[170] ***Opera 6.06 released with same vulnerability***[171]	**Multiple**	**Opera Web Browser 6.0.5 win32, 7.0 win32 Beta 1&2**	**A buffer overflow vulnerability exists when an URL is submitted that contains a specially crafted, long username, which could let a remote malicious user execute arbitrary instructions.** ***Opera 6.06 has been released with this same vulnerability.***	**Upgrade available at:** **http://www.opera.com/download/index.dml?opsys=Windows&lng=en&platform=Windows**	**Opera Username Remote Buffer Overflow**	**High**	**Bug discussed in newsgroups and websites. Proofs of Concept exploit scripts have been published.**
osCommerce[172]	Windows, Unix	OsCommerce 2.1, 2.2ms1	Multiple Cross-Site Scripting vulnerabilities exist in numerous scripts due to insufficient filtering of URI parameters, which could let a remote malicious user execute arbitrary HTML and script code.	The vendor has reportedly issued a fixed version, available via CVS: http://www.oscommerce.com/downloads/snapshot	OSCommerce Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
PHP[173]	MacOS X 10.X, Unix	PHP 4.0-4.0.7, 4.1.0-4.1.2, 4.2.0-4.2.3, 4.3, 4.3.1	Several vulnerabilities exist: a vulnerability exists in the socket_recv() function due to insufficient sanitization of user-supplied argument values, which could let a malicious user cause a Denial of Service and possibly execute arbitrary code; a vulnerability exists in the socket_recvfrom() function due to insufficient sanitization of user-supplied argument values, which could let a malicious user cause a Denial of Service and possibly execute arbitrary code; and a vulnerability exists in the emalloc() function due to insufficient boundary checking, which could let a malicious user corrupt memory.	No workaround or patch available at time of publishing.	PHP socket_recv(), socket_recvfrom(), & emalloc() Vulnerabilities	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
PHP[174]	MacOS X 10.x, Unix	PHP 4.1.0-4.1.2, 4.2.0-4.2.3, 4.3, 4.3.1	A buffer overflow vulnerability exists in 'STR_Repeat,' which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PHP STR_Repeat Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[170] SecurityFocus, February 10, 2003.
[171] SecurityFocus, March 20, 2003.
[172] iProyectos Security Advisory, March 20, 2003.
[173] @(#) Mordred Security Labs Advisory, March 26, 2003.
[174] @(#) Mordred Security Labs Advisory, April 1, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
PHP Arena[175]	Unix	paFileDB 3.0, 3.0 Beta, 3.1	Multiple vulnerabilities exist in the paFileD file manage script due to insufficient sanitization of user-supplied URI parameters, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	PAFileDB. PHP Input Validation	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
PHP Group[176]	Unix	PHP 4.3.1	A buffer overflow vulnerability exists in the openlog() function, which could let a malicious user cause a Denial of Service and possibly execute arbitrary commands.	No workaround or patch available at time of publishing.	PHP openlog() Buffer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
PHP Group [177]	Unix	PHP 4.3, 4.3.1	A vulnerability exists in the socket_iovec_alloc() function due to a failure to carry out sanity checks on user-supplied argument values, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.	No workaround or patch available at time of publishing.	PHP socket_iovec_alloc() Integer Overflow	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit has been published.
PostNuke Development Team[178]	Unix	PostNuke 0.721, PostNuke Phoenix 0.722, 0.72	Multiple path disclosure vulnerabilities exist in various PHP scripts due to insufficient error handling, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	PostNuke Sensitive Information Disclosure	Medium	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
ProtWare Inc.[179]	Windows	HTML Guardian 6.3	A vulnerability exists in the encryption scheme, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	ProtWare HTML Guardian Encryption	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Qual-comm[180], [181] ***SuSE issues upgrade*** [182]	**Unix**	**qpopper 4.0.1**	**A vulnerability exists when the 'mdef' command is called and a malicious macro name is supplied, which could let a remote malicious user execute arbitrary code.**	**Upgrade available at:** **ftp://ftp.qualcomm.com/eudora/servers/unix/popper/beta** **Debian:** http://security.debian.org/pool/updates/main/q/qpopper/ ***SuSE:*** **ftp://ftp.suse.com/pub/suse**	**Qpopper Remote Memory Corruption**	**High**	**Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.**

[175] Flurnet Security Advisory, March 23, 2003.
[176] @(#) Mordred Security Labs Advisory, March 27, 2003.
[177] @(#) Mordred Security Labs Advisory, March 25, 2003.
[178] Securiteam, March 26, 2003.
[179] Bugtraq, March 20, 2003.
[180] Bugtraq, March 10, 2003.
[181] Debian Security Advisory, DSA-259-1, March 12, 2003.
[182] SuSE Security Announcement, SuSE-SA:2003:018, March 21, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Real Networks[183]	Windows 95/98/ME/ NT 4.0/2000, XP, MacOS X, Unix	RealOne Enterprise Desktop 6.0.11.774, RealOne Player 9.0.0.297 for OS X, 9.0.0.288 for OS X, 6.0.11.853, 6.0.11.841, 6.0.11.830, 6.0.11.818, 2.0, Gold for Windows 6.0.10 .505, 8.0 Win32, 8.0 Unix, 8.0 Mac	A buffer overflow vulnerability exists in a data compression library used to process PNG images, which could let a remote malicious user execute arbitrary code.	Updates available at: http://service.real.com/help/faq/security/securityupdate_march2003.htm	RealPlayer Buffer Overflow PNG Images CVE Name: CAN-2003-0141	High	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
RedHat[184]	Unix	RedHat Linux 9.0 i386	A vulnerability exists in 'vsftpd' because it was improperly compiled, which could let a remote malicious user obtain bypass security restrictions.	Upgrade available at: ftp://updates.redhat.com/9/en/os/i386/vsftpd-1.1.3-8.i386.rpm	Red Hat Linux 9 vsftpd Compiling Error CVE Name: CAN-2003-0135	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
rxvt[185] ***Vendors release upgrades[186, 187]***	**Unix**	**rxvt 2.6.1-2.7.8**	**A vulnerability exists in the window title reporting feature, which could let a malicious user execute arbitrary commands.**	***RXVT:*** **ftp://ftp.rxvt.org/pub/rxvt/rxvt-2.7.10.tar.gz** ***RedHat:*** **ftp://updates.redhat.com/** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php**	**RXVT Window Title Reporting Escape Sequence Command** **CVE Name: CAN-2003-0066**	**High**	**Bug discussed in newsgroups and websites. There is no exploit code required.**
rxvt[188] ***Vendors release upgrades[189, 190]***	**Unix**	**rxvt 2.6.1-2.7.8**	**A vulnerability exists because a screen dump feature may be abused to corrupt local files that which are writeable by the terminal user, which could let a local/remote malicious user obtain elevated privileges.**	***RXVT:*** **ftp://ftp.rxvt.org/pub/rxvt/rxvt-2.7.10.tar.gz** ***RedHat:*** **ftp://updates.redhat.com/** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php**	**RXVT Screen Dump Escape Sequence Local File Corruption** **CVE Name: CAN-2003-0022**	**Medium**	**Bug discussed in newsgroups and websites. There is no exploit code required.**

[183] Core Security Technologies Advisory, CORE-2003-0306, March 28, 2003.
[184] Red Hat Security Advisory, RHSA-2003:084-01, April 1, 2003.
[185] Bugtraq, February 24, 2003.
[186] Red Hat Security Advisory, RHSA-2003:054-00, March 17, 2003.
[187] Mandrake Linux Security Update Advisory, MDKSA-2003:034, March 25, 2003.
[188] Bugtraq, February 24, 2003.
[189] Red Hat Security Advisory, RHSA-2003:054-00, March 17, 2003.
[190] Mandrake Linux Security Update Advisory, MDKSA-2003:034, March 25, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
rxvt[191] ***Vendors release upgrades*** [192, 193]	**Unix**	**rxvt 2.6.1-2.7.9**	**A vulnerability exists in the MenuBar feature, which could let a malicious user execute arbitrary commands.**	***RXVT:*** **ftp://ftp.rxvt.org/pub/rxvt/rxvt-2.7.10.tar.gz** ***RedHat:*** **ftp://updates.redhat.com/** ***Mandrake:*** **http://www.mandrakesecure.net/en/ftp.php**	**RXVT Menu Bar Escape Sequence Command Execution** **CVE Name: CAN-2003-0023**	**High**	**Bug discussed in newsgroups and websites. There is no exploit code required.**
Sambar Technologies [194]	Windows 95/98/ME/ NT 4.0/2000, XP	Sambar Server 5.1, 5.2, 5.2 b, 5.3 b4	Multiple vulnerabilities exist: an information disclosure vulnerability exists in 'testcgi.exe' and 'environ.pl,' which could let a remote malicious user obtain sensitive information; a Directory Traversal vulnerability exists in 'iecreate,stm' and 'ieedit.stm' due to improper validation of URL requests, which could let a remote malicious user obtain sensitive information; and multiple Cross-Site Scripting vulnerabilities exist in numerous scripts due to inadequate filtering of HTML code, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	Sambar Server Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published for the information disclosure vulnerability. Directory Traversal vulnerability and Cross-Site Scripting vulnerabilities can be exploited via a web browser.
Samba-TNG[195]	Unix	Samba-TNG 0.3	A privilege escalation vulnerability exists, which could let a remote malicious user obtain root privileges.	Upgrade available at: http://www.samba-tng.org/download/tng/	Samba-TNG Remote Root Privileges	**High**	Bug discussed in newsgroups and websites.
SAP[196]	Unix	DB 7.3.00, 7.4	A vulnerability exists because the 'dbmsrv' and 'lserver' binaries are installed with insecure permissions, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	SAP DB RPM Install World Writable Binary	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[191] Bugtraq, February 24, 2003.
[192] Red Hat Security Advisory, RHSA-2003:054-00, March 17, 2003.
[193] Mandrake Linux Security Update Advisory, MDKSA-2003:034, March 25, 2003.
[194] Security Corporation Security Advisory, SCSA-012, March 27, 2003.
[195] Bugtraq, March 23, 2003.
[196] Secure Network Operations, Inc. Advisory, SRT2003-03-31-1219, March 31, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Scott Barr[197]	Windows, Unix	ScozBook 1.1 BETA	Several vulnerabilities exist: a vulnerability exists in the 'add.php' script due to insufficient HTML filtering, which could let a remote malicious user execute arbitrary code; and a path disclosure vulnerability exists in the 'view.php3'script, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	ScozBook HTML Injection	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. There is no exploit code required for the 'add.php' vulnerability. Proof of Concept exploit has been published for the 'view.php3' vulnerability.
Seagull Software[198]	Windows NT 4.0	J walk 3.2c9	A Directory Traversal vulnerability exists due to improper sanitization of web requests, which could let a remote malicious user obtain sensitive information.	Contact the vendor for upgrade information.	JWalk Application Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Snort Project[199]	Windows, Unix	Snort 1.9.1	A vulnerability exists in the default 'snort.conf' configuration because certain types of packets are not detected, which could let a remote malicious user submit specially crafted packets that bypass scanning.	Upgrade available at: http://www.snort.org/dl/snort-2.0.0rc1.tar.gz	Snort Evasion Scan	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Stefan Bethge[200]	Multiple	nflash 0.7, 0.7.1	Vulnerabilities exist due insufficient sanitization of user-supplied input that is used to generate pages with dynamic content, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	NFlash Useradmin. CGI Script Code Injection	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Sun Micro-systems, Inc.[201]	Unix	Solaris 2.5.1, 2.5.1_x86, 2.5.1 _ppc, 2.6, 2.6_x86, 7.0, 7.0_x86	A buffer overflow vulnerability exists in the 'lpstat' utility, which could let a malicious user obtain root privileges.	Patches available at: http://sunsolve.Sun.COM/pub-cgi/retrieve.pl?doc=fsalert/52443 Patch 106236-12, Patch 106235-12, Patch 107116-12, Patch 107115-12	Solaris lpstat Buffer Overflow CVE Name: CAN-2003-0091	**High**	Bug discussed in newsgroups and websites.
Sun Micro-systems, Inc.[202]	Unix	Solaris 9.0, 9.0_x86	A vulnerability exists in the newtask(1) command, which could let a malicious user obtain elevated privileges.	Patches available at: http://sunsolve.sun.com/pub-cgi/findPatch.pl?patchId=114714&rev=01	Solaris NewTask Privilege Elevation	Medium	Bug discussed in newsgroups and websites.

[197] Bugtraq, March 29, 2003.
[198] IRM Security Advisory No. 005, March 25, 2003.
[199] Secunia Security Advisory, March 28, 20093.
[200] SecurityFocus, March 26, 2003.
[201] NSFOCUS Security Advisory, SA2003-02, March 31, 2003.
[202] Sun(sm) Alert Notification, 52111, March 28, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sun Microsystems, Inc.[203] ***Sun issues patch***[204]	**Windows NT 4.0/2000**	**ONE Application Server 6.0, 6.5**	**A buffer overflow vulnerability exists in the Connector Module, a Netscape Server Application Programming Interface (NSAPI) plug-in, which could let a remote malicious user execute arbitrary code.**	***Patch/workaround/ upgrade available at:*** **http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F52022**	**ONE Application Server Connector NSAPI Module Remote Buffer Overflow** **CVE Name: CAN-2002-0387**	**High**	**Bug discussed in newsgroups and websites.** **Vulnerability has appeared in the press and other public media.**
Sun Microsystems, Inc.[205] ***Sun issues workaround***[206]	**Unix**	**SUN Wllдap 11.8**	**A buffer overflow vulnerability exists in the SUNWlldap library when an application linked to the LDAP library is used to resolve hostnames of excessive length, which could let a malicious user execute arbitrary code.**	***Workaround available at:*** **http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F52222**	**Sun SUNWlldap Library Buffer Overflow**	**High**	**Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.**
Symantec[207]	Windows NT 4.0/2000, Unix	Enterprise Firewall 7.0 Solaris, 7.0 NT/2000	A vulnerability exists because URL encoding techniques can be used to bypass blocking mechanisms, which could let a remote malicious user bypass security restrictions.	Symantec has a Support article outlining procedures to protect against this weakness. See the link to "How to protect against directory traversal and URL overflow attacks" available at: http://service1.symantec.com/SUPPORT/ent-gate.nsf/docid/2003032507434754	Enterprise Firewall HTTP Blocking Bypass CVE Name: CAN-2003-0106	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
VChat[208]	Unix	VChat 2.0	A vulnerability exists due to a failure to protect chat session logs, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	VChat Message Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Web Drive Limited[209]	Windows, Unix	PHP WEB CHAT 2.0	Cross-Site Scripting vulnerabilities exists in the 'register.php,' 'login.php,' and 'profile.php' scripts due to insufficient filtering of HTML code from user-supplied input, which could let a remote malicious user execute arbitrary HRML code.	No workaround or patch available at time of publishing.	Web Chat Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Proof of Concept has been published.

[203] @stake, Inc. Security Advisory, A031303-1, March 13, 2003.
[204] Sun(sm) Alert Notification, 52022, March 24, 2003.
[205] Securiteam, March 16, 2003.
[206] Sun(sm) Alert Notification, 52222, March 26, 2003.
[207] Corsaire Security Advisory, March 26, 2003.
[208] Bugtraq, March 23, 2003.
[209] Secunia Security Advisories, March 27, 2003.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Ximian[210, 211]	Unix	Evolution 1.0.3-1.0.8, 1.1.1, 1.2-1.2.2	Multiple vulnerabilities exist: a remote Denial of Service vulnerability exists in the parsing component when a malicious user includes a specially crafted UUE header as part of an e-mail; a remote Denial of Service vulnerability exists in the Mail User Agent (MUA) when a malicious user submits a specially encoded e-mail message; and a vulnerability exists due to insufficient validation of MIME image/* Content-Type fields, which could let a remote malicious user execute arbitrary code or bypass the "Don't connect to remote hosts to fetch images" option.	**RedHat:** ftp://updates.redhat.com/	Evolution Multiple Remote Vulnerabilities CVE Name: CAN-2003-0128, CAN-2003-0129, CAN-2003-0130	Low/ Medium/ **High** **(Low if a DoS; Medium if security policies can be bypassed; and High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
Xoops[212]	Windows, Unix	Xoops 2.0	A vulnerability exists in the "$xoopsOption" variable, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	XOOPS XoopsOption Information Disclosure	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

[210] Core Security Technologies Advisory, CORE-20030304-01, March 19, 2003.
[211] Red Hat Security Advisory, RHSA-2003:108-01, March 21, 2003.
[212] Security Corporation Security Advisory, SCSA-011, March 20, 2003.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between March 19 and April 3, 2003, listed by date of script, script names, script description, and comments. Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing. During this period, 30 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script Name	Script Description
April 3, 2003	Vncpwdump-src-1_0_0.zip	VNCPwdump can be used to dump and decrypt the registry key containing the encrypted VNC password in a few different ways.
April 3, 2003	Safemode-adv-chitext.txt	A utility used to put Chinese Big5 codes in TeX/LaTeX documents that contains two setuid root binaries that execute cat without using an explicit path allowing an malicious user to easily gain root privileges.
April 3, 2003	0x82-Remote.Passlogd_Sniff.Xpl.c	Remote exploit for the passlogd buffer overflow vulnerability.
April 3, 2003	Passifist_src_1.0.0.tgz	A tool for passive network discovery that can be used for a number of different things, but was mainly written to discover hosts without actively probing a network. It analyzes broadcast traffic and has a plugin architecture through which it dissects and reports services found.
April 2, 2003	Rpcexp.c	Script that exploits the Windows 2000 RPC Service Remote Denial of Service vulnerability.
April 2, 2003	Openfuckv2.c	Remote exploit for Apache + OpenSSL v0.9.6d and below vulnerability.
April 1, 2003	Ptrace-kmod.c	Script that exploits the Linux Kernel Root Access vulnerability.
April 1, 2003	Recluse.pl	A web spidering utility written in Perl that takes a host as input along with a document path.
April 1, 2003	Printerfun.pl	A utility that allows a remote user to change the "ready message" on printers that support PJL commands.
April 1, 2003	Cgrep.c	A utility that works like grep but was designed to be used against core files.
April 1, 2003	Alcatel-ex.c	A utility that extracts files from the ramdisk image located in Alcatel speedtouch home/pro modems.
April 1, 2003	Fuckptrace.c	A Linux kernel module used for bypassing anti-ptrace protection used against the reverse engineering process.
April 1, 2003	Nfbypass.c	A Linux kernel module for the 2.4.x series that will bypass netfilter rules.
March 31, 2003	Rs_iis_xpl.pl	Perl script that exploits the Windows 2000 WebDAV Remote Buffer Overflow vulnerability.
March 28, 2003	Rs_iis.c	Proof of concept exploit for the Windows 2000 WebDAV Buffer Overflow vulnerability.
March 28, 2003	**Gespuis.c**	**An irc bouncer that exploits BitchX/Epic vulnerability.**
March 28, 2003	**Ftpd.pl**	**Perl script that exploits the CuteFTP Buffer Overflow vulnerability.**

Date of Script (Reverse Chronological Order)	Script Name	Script Description
March 28, 2003	Patch-opensshhack-1.2.tgz	Backdoor patch for OpenSSH 3.2.2p1 that allows for a universal password for all accounts so that a universal user that can impersonate an existing account and disable all related logging facilities for the session.
March 27, 2003	Wd.pl	Perl script that exploits the Microsoft Ntdll.dll vulnerability.
March 27, 2003	Elfsh-0.5b6-Pre1-LINUX.Tgz	An interactive and scriptable reverse engineering tool with advanced read/write capabilities for the ELF format.
March 26, 2003	**Nestea.c**	**Script that exploits the DI-614+ IP Remote Denial of Service vulnerability.**
March 25, 2003	Nessus-2.0.1.tar.gz	A free, up-to-date full featured remote security scanner for Linux, BSD, Solaris and some other systems that is multithreaded, plugin-based, has a nice GTK interface, and currently performs over 920 remote security checks.
March 24, 2003	Wb.c	Script that exploits the Microsoft NTdll.dll vulnerability.
March 24, 2003	**Isec-options.c**	**Script that exploits the SuperStack II RAS 1500 Malicious IP Header Denial of Service & Inadequate Authentication vulnerabilities.**
March 24, 2003	Lprmexp.c	Script that exploits the Multiple Vendor LPRM Buffer Overflow vulnerability.
March 24, 2003	Lprm-bsd.c	Script that exploits the Multiple Vendor LPRM Buffer Overflow vulnerability.
March 21, 2003	Eddos.zip	Exploit for the eDonkey Clients Multiple Chat Dialog Denial of Service vulnerability and Emule Empty Nickname Chat Request Remote Denial Of Service vulnerability.
March 21, 2003	**Ipaq_crash.c**	**Script that exploits the Microsoft ActiveSync Remote Denial Of Service vulnerability.**
March 20, 2003	**Protpop.pl**	**Perl script that exploits the ProtWare HTML Guardian Encryption vulnerability.**
March 19, 2003	Ptwebdav.zip	A utility for Windows that checks for IIS 5.0 servers which are vulnerable to the WebDAV Vulnerability.

Trends

- **The number of security events detected by companies in the first quarter of 2003 jumped nearly 84 percent over the preceding three months. The increase in events, which can include minor probes for holes in network security as well as major attacks, stems mainly from an increase in worms and automated attack software.**
- Over the past few weeks, their have been an increased number of reports of intruder activity involving the exploitation of Null (i.e., non-existent) or weak Administrator passwords on Server Message Block (SMB) file shares used on systems running Windows 2000 or Windows XP. This activity has resulted in the successful compromise of thousands of systems, with home broadband users' systems being a prime target. Recent examples of such activity are the attack tools known as W32/Deloder, GT-bot, sdbot, and W32/Slackor. For more information, see CERT® Advisory CA-2003-08, located at: http://www.cert.org/advisories/CA-2003-08.html.
- **The Department of Homeland Security (DHS), National Infrastructure Protection Center (NIPC) has issued an advisory to heighten awareness of the recently discovered Remote SendMail Header Processing Vulnerability (CAN-2002-1337). NIPC has been working closely with the industry on vulnerability awareness and information dissemination. For more information, see 'Bugs, Holes & Patches' table and DHS/NIPC Advisory 03-004 located at: http://www.nipc.gov/warnings/advisories/2003/03-004.htm.** ***Note: SendMail is the most commonly used Mail Transfer Agent and processes an estimated 50 to 75 percent of all Internet e-mail traffic. System administrators should be aware that many SendMail***

***servers are not typically shielded by perimeter defense applications.* Remote malicious users may gain access to other systems through a compromised SendMail server, depending on local configurations.**

- Systems are being compromised through the exploitation of null or weak default 'sa' passwords in Microsoft SQL Server and Microsoft Data Engine.
- Propagation of SQL 'Slammer' or 'Sapphire' malicious code is still causing varied levels of network degradation across the Internet and the compromise of vulnerable machines.
- NIPC has issued an advisory regarding the propagation of an SQL worm. The self-propagating malicious code exploits multiple vulnerabilities in the Resolution Service of Microsoft SQL Server 2000. This worm activity appears to have caused various levels of network degradation across the Internet. In addition to the compromise of vulnerable machines; the apparent effects of this fast-spreading, virus-like infection has overwhelmed the world's digital pipelines and interfered with Web browsing and delivery of e-mail. For more information, see Virus Section, WORM_SQLP1434.A description and NIPC Advisory 03-001.1, located at: http://www.nipc.gov/warnings/advisories/2003/03-001.1updates.htm. For patch information, see:
  - http://www.microsoft.com/security/slammer.asp
  - http://www.microsoft.com/technet/security/bulletin/MS02-061.asp
  - http://www.microsoft.com/technet/security/bulletin/MS02-039.asp
- The CERT/CC has released an advisory regarding a buffer overflow vulnerability in the Microsoft Windows Shell. For more information, see Bugs, Holes & Patches table entry, "Windows XP WMA/MP3 Buffer Overflow" and CERT® Advisory CA-2002-37, located at: http://www.cert.org/advisories/CA-2002-37.html.
- The CERT/CC has released an advisory regarding multiple vendors' implementations of the secure shell (SSH) transport layer protocol contain vulnerabilities that could allow a remote malicious user to execute arbitrary code with the privileges of the SSH process or cause a denial of service. The vulnerabilities affect SSH clients and servers, and they occur before user authentication takes place. For more information, see Bugs, Holes & Patches table entry "Multiple Vendor SSH2 Implementation" and CERT® Advisory CA-2002-36, located at: http://www.cert.org/advisories/CA-2002-36.html.
- The CERT/CC has received reports of increased scanning for NetBIOS services. Probes to port 137/udp may be indicative of such activity.

Viruses

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. **To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available**. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. Following this table are descriptions of new viruses and updated versions discovered in the last two weeks. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

Ranking	Common Name	Type of Code	Trends	Date
1	W32/Klez	Worm	Stable	January 2002
2	W32/Yaha	Worm	Increase	February 2002
3	W32/Sobig	Worm	Stable	January 2003
4	W32/Bugbear	Worm	Decrease	September 2002
5	W32/Avril	Worm	Slight Decrease	January 2003
6	JS/NoClose	Trojan	Stable	May 2002
7	Elkern	File Infector	Stable	October 2001
8	Funlove	File	Stable	November 1999
9	W32/SQLSlammer	Worm	Slight Increase	January 2003
10	CodeRed	Worm	New to Table	July 2001

Note: Virus reporting may be weeks behind the first discovery of infection. A total 202 distinct viruses are currently considered "in the wild" by anti-virus experts, with another 319 viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

VBS.Alcaul.B@mm (Alias: I-Worm.Alcaul.o) (Visual Basic Script Worm): This is a worm that sends itself to all the contacts in the Microsoft Outlook Address Book. The email that the worm sends has the following characteristics:

- Subject: ***Wow Found Binladen****
- Attachment: Random name with .vbs file extension

VBS.Alcaul.B@mm adds a macro to the Microsoft Word Normal template causing other Word documents to become infected.

VBS.Ereglili@mm (Visual Basic Script Worm): This is a worm that sends itself to all the contacts in the Microsoft Outlook Address Book. The e-mail that the worm sends has the following characteristics:

- Subject: A$k ve Gozyasi
- Attachment: Ask.vbs

The worm will copy itself to various folders and overwrites files.

VBS_LISA.A (Aliases: VBS.Lisa.A@mm, VBS.Charlene) (Visual Basic Script Worm): This Visual Basic Script (VBScript) worm infects files with VBS and VBE extensions in all drives. It propagates through Microsoft Outlook, KaZaA, and mIRC. It arrives via e-mail in an HTML-based e-mail message with the following details:

- Subject: Click YES and vote against war!

The worm e-mail message does not contain the worm as an attachment, but rather it is embedded as a script in the e-mail itself. It sends this e-mail message to all contacts in the Microsoft Outlook address book. This worm deletes .DOC files and certain critical system files such as WIN.COM and REGEDIT.EXE. In addition, it creates up to 5,000 folders and non-malicious text files, downgrading system performance. Additionally, it hides the desktop icons and formats drive C on machines running Windows 98 or ME. This VBScript file infector worm runs on systems that have the Windows Scripting Host installed.

VBS.SST.B@mm (Visual Basic Script Worm): This is a Visual Basic Script (VBS) worm that uses Microsoft Outlook to send itself to all the contacts in the Outlook Address Book. The e-mail has the following characteristics:

- Subject: Your file
- Attachment: Untitled.vbs

VBS.SST.B@mm also attempts to spread itself through the KaZaA, KaZaA Lite, Bearshare, Morpheus, and Grokster file-sharing networks, as well as through mIRC and ICQ.

W32/Cult-A (Aliases: WORM_CULT.A, Win32/Cult.A@mm, W32.HLLW.Cult@mm) (Win32 Worm): This non-memory resident worm propagates via the KaZaA peer-to-peer file-sharing network. It also e-mails copies of itself to addresses with the following domains: e-mail.com, Earthlink.net, Roadrunner.com, yahoo.com, msn.com, and hotmail.com. It sends e-mail with the following format:

- Subject: Hi, I sent you an eCard from BlueMountain.com
- Attachment: BlueMountaineCard.pif

It spoofs the from field on its e-mail messages, randomly selecting from a list of 94 strings in its body. This worm, which runs on Windows 95, 98, ME, NT, 2000, and XP, drops a backdoor, BKDR_CULT.A.

W32/Cult-B (Alias: I-Worm.Cult-B, W32/Lanet@mm, Win32.Cult.B, W32/BlueECard@MM) (Win32 Worm): This worm spreads via file sharing on KaZaA networks and by e-mailing itself to random e-mail addresses. The e-mail has the following characteristics:

- Subject line: Hi, I sent you an eCard from BlueMountain.com
- Attached file: BlueMountaineCard.pif

When first run, the worm moves itself to the Windows system folder as “wuauqmr.exe” and creates the registry entries so that “wuauqmr.exe” is run automatically each time Windows is started:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\NvCpTDaemon = wuauqmr.exe
- HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce\NvCpTDaemon = wuauqmr.exe

The worm creates the folder “jdfghtrg” in the Windows system folder and copies itself to this folder using various filenames. The worm makes the “jdfghtrg” folder shareable on KaZaA networks by creating the registry entry:

- HKCU\Software\Kazaa\LocalContent\Dir0 = 012345:%SYSTEM%\jdfghtrg\

Each time the worm is run, it performs a Denial-of-Service attack on either www.chat-planet.nl or chat.planet.nl by repeatedly creating and destroying connections to the chosen site.

W32/Frethem-T (Alias: WORM_FRETHEM.P) (Win32 Worm): W32/Frethem-T is similar to W32/Frethem-B. One difference is the addition of limited backdoor capabilities.

W32.HLLW.Cult.C@mm (Win32 Worm): This is an e-mail worm that has backdoor capabilities. It uses its own SMTP engine to send itself to randomly generated recipient names at these domains: e-mail.com, earthlink.net, roadrunner.com, yahoo.com, msn.com, and hotmail.com. The e-mail message has the following characteristics:

- Subject: Hi, I sent you an eCard from BlueMountain.com
- Attachment: BlueMountaineCard.pif

This threat is compressed with ASPack.

W32.HLLW.Suava (Win32 Worm): This worm has two components:

- A file that downloads the worm/backdoor from a Web site
- The worm/backdoor itself

The downloader downloads a file from a Web site to %Windir%\Fb.exe, and then executes that file. It also creates a copy of the downloaded file as C:\Windows\Mspread.exe. W32.HLLW.Suava attempts to spread to the network shares.

W32.Kwbot.E.Worm (Win32 Worm): W32.Kwbot.E.Worm attempts to spread across the file-sharing networks, such as KaZaA and iMesh. The worm also has a Backdoor Trojan capability that allows a malicious user to control your computer. It is packed with ASPack v2.12 and is a variant of W32.Kwbot.Worm.

W32.Sahay.C@mm (Win32 Worm): This is a mass-mailing worm that uses Microsoft Outlook to spread itself to all the contacts in the Outlook Address Book. The e-mail has the following characteristics:

- Subject: Fw: Sit back and be surprised.
- Attachment: MathMagic.scr

The worm attempts to prepend itself to all the .exe files that it finds in the \Windows folder and in the C:\Program Files\Mirc\Download folder. Due to bugs in the worm's code, this threat may crash the computer or corrupt files in these folders. Then, the worm will restart the computer.

W32/Trab.worm (Win32 Worm): This is a floppy worm. When run, the worm copies itself to C:\WINDOWS\SYSTEM\W16OFF.exe and creates the following registry key in order to run at Windows start up:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "Spool32" = C:\WINDOWS\SYSTEM\W16OFF.exe

Every 2-3 minutes, the worm copies itself to floppy drive A:. It creates the following files:

- A:\command.com - the worm itself.
- C:\WINDOWS\SYSTEM\HTA.doc - word document.
- A:\TRAP.doc - same word document.
- C:\listf.vxd - a log file.

W32.Yaha.Q@mm (Aliases: W32.Yaha.I@mm, I-Worm.Lentin.i, W32/Yaha.gen@MM) (Win32 Worm): This is a worm that is a variant of W32.Yaha.K@mm. The difference between the variants are that W32.Yaha.Q@mm is packed using ASPack, which is a different packer than that used to pack W32.Yaha.K@mm. W32.Yaha.Q@mm terminates some antivirus and firewall processes. It uses its own SMTP engine to e-mail itself to all the contacts in the Windows Address Book, MSN Messenger, .NET Messenger, Yahoo Pager, and all the files whose extensions contain the letters HT. The e-mail message has randomly chosen the subject line, message, and attachment name. This threat is written in the Microsoft C++ programming language.

W97M.Ashraf (Word 97 Macro Virus): This is a macro virus that spreads by infecting all the active Word documents, as well as all the Word documents located in your Microsoft Word template folder. When a document is opened or closed W97M.Ashraf does the following:

- Copies the macro Mxfile into all the active Word documents.
- Copies the macro Mxfile into all the documents located in your Microsoft Word template folder.

W97M.Twopey.D (Alias: W97M.Virugoer) (Word 97 Macro Virus): This is a macro virus that infects Microsoft Word documents. It infects the Microsoft Word template file, Normal.dot, and uses it to spread the virus to other Word documents. On Windows 95/98/ME, W97M.Twopey.D may overwrite the Autoexec.bat file with a new malicious file.

WORM_BIBROG.E (Alias: Win32/Bibrog.E@mm) (Win32 Worm): This memory-resident worm propagates via e-mail and via peer-to-peer file-sharing networks, such as KaZaA and Morpheus. It drops copies of itself in the following shared folders of popular P2P file-sharing applications:

- KaZaa\My shared Folder
- ICQ\Shared
- Grokster\My Grokster
- Morpheus\My Shared Folder

It propagates via e-mail by sending out copies of itself attached on e-mail with the following details to all addresses in the Windows Address Book:

- Subject: Fwd: La Academia Azteca
- Attachment: academia.exe

This worm, which runs on Windows 95, 98, ME, NT, 2000, and XP, displays a shooting game to hide its malicious intent.

WORM_LOVGATE.G (W32 Worm): This memory-resident worm is an exact replica of WORM_LOVGATE.F except for the name of the event that it creates to indicate memory-residency. It is ASPack-compressed and propagates through network shares by dropping copies of itself to shared folders with read/write access. The files that it drops can have various names. This worm also propagates via e-mail by replying to all new messages received in Microsoft Outlook and Outlook Express and gathers target e-mail addresses from HTML files that it finds in the current, Windows, and My Documents folders and sends an e-mail message with itself as attachment to all the said e-mail addresses. This malware runs on Windows 95, 98, ME, NT, 2000 and XP.

XM97/Morx-A (Aliases: X97M.Romlax, X97M_MORX.A, X97M/Morx, Macro.Excel97.Morx) (Excel 97 Macro Virus): This virus has been reported in the wild. It is activated when Excel workbooks are opened. XM97/Morx-A will create the file rom.xla in the following folder:

- C:\Program Files\Microsoft Office\Office\Library\Analysis

and add itself as an Add-In called "Rom." This can be seen from the Tools\Add-Ins display of Microsoft Excel.

X97M.Phoneman (Excel 97 Macro Virus): This is a macro virus that infects files when they are closed.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. Note: At times, Trojans may contain names or content that may be considered offensive.

Trojan	Version	CyberNotes Issue #
AdwareDropper-A	A	CyberNotes-2003-04
AIM-Canbot	**N/A**	**Current Issue**
Backdoor.Acidoor	N/A	CyberNotes-2003-05
Backdoor.Amitis	N/A	CyberNotes-2003-01
Backdoor.Assasin.D	D	CyberNotes-2003-01
Backdoor.Assasin.E	E	CyberNotes-2003-04
Backdoor.Beasty	N/A	CyberNotes-2003-02
Backdoor.Beasty.B	B	CyberNotes-2003-03
Backdoor.Beasty.C	C	CyberNotes-2003-05
Backdoor.Beasty.D	D	CyberNotes-2003-06
Backdoor.Beasty.E	E	CyberNotes-2003-06
Backdoor.Bmbot	N/A	CyberNotes-2003-04
Backdoor.Bridco	N/A	CyberNotes-2003-06
Backdoor.CHCP	N/A	CyberNotes-2003-03
Backdoor.Colfuser	N/A	CyberNotes-2003-01
Backdoor.Cow	N/A	CyberNotes-2003-01
Backdoor.Cybspy	N/A	CyberNotes-2003-01
Backdoor.Dani	N/A	CyberNotes-2003-04
Backdoor.Darmenu	N/A	CyberNotes-2003-05
Backdoor.Deftcode	N/A	CyberNotes-2003-01
Backdoor.Delf.F	**F**	**Current Issue**
Backdoor.Drator	N/A	CyberNotes-2003-01

Trojan	Version	CyberNotes Issue #
Backdoor.Dvldr	N/A	CyberNotes-2003-06
Backdoor.Fluxay	**N/A**	**Current Issue**
Backdoor.FTP.Casus	N/A	CyberNotes-2003-02
Backdoor.FTP_Ana.C	**N/A**	**Current Issue**
Backdoor.Graybird	**N/A**	**Current Issue**
Backdoor.HackDefender	N/A	CyberNotes-2003-06
Backdoor.Hethat	N/A	CyberNotes-2003-01
Backdoor.Hipo	N/A	CyberNotes-2003-04
Backdoor.Hitcap	N/A	CyberNotes-2003-04
Backdoor.Hornet	N/A	CyberNotes-2003-01
Backdoor.IRC.Aladinz	N/A	CyberNotes-2003-02
Backdoor.IRC.Cloner	N/A	CyberNotes-2003-04
Backdoor.IRC.Yoink	N/A	CyberNotes-2003-05
Backdoor.IRC.Zcrew	N/A	CyberNotes-2003-04
Backdoor.Khaos	N/A	CyberNotes-2003-04
Backdoor.Kilo	N/A	CyberNotes-2003-04
Backdoor.Kol	N/A	CyberNotes-2003-06
Backdoor.Krei	N/A	CyberNotes-2003-03
Backdoor.Lala	N/A	CyberNotes-2003-01
Backdoor.LittleWitch.C	C	CyberNotes-2003-06
Backdoor.Longnu	N/A	CyberNotes-2003-06
Backdoor.Marotob	N/A	CyberNotes-2003-06
Backdoor.Massaker	N/A	CyberNotes-2003-02
Backdoor.MSNCorrupt	N/A	CyberNotes-2003-06
Backdoor.NetDevil.B	B	CyberNotes-2003-01
Backdoor.NetTrojan	N/A	CyberNotes-2003-01
Backdoor.Ohpass	N/A	CyberNotes-2003-01
Backdoor.OICQSer.165	N/A	CyberNotes-2003-01
Backdoor.OICQSer.17	17	CyberNotes-2003-01
Backdoor.Optix.04.d	04.d	CyberNotes-2003-04
Backdoor.OptixDDoS	**N/A**	**Current Issue**
Backdoor.OptixPro.10.c	10.c	CyberNotes-2003-01
Backdoor.OptixPro.12.b	**12.b**	**Current Issue**
Backdoor.Plux	N/A	CyberNotes-2003-05
Backdoor.PSpider.310	310	CyberNotes-2003-05
Backdoor.Queen	N/A	CyberNotes-2003-06
Backdoor.Redkod	N/A	CyberNotes-2003-05
Backdoor.Remohak.16	16	CyberNotes-2003-01
Backdoor.RemoteSOB	N/A	CyberNotes-2003-01
Backdoor.Rephlex	N/A	CyberNotes-2003-01
Backdoor.Rsbot	**N/A**	**Current Issue**
Backdoor.SchoolBus.B	B	CyberNotes-2003-04
Backdoor.Sdbot.C	C	CyberNotes-2003-02
Backdoor.Sdbot.D	D	CyberNotes-2003-03
Backdoor.Sdbot.E	E	CyberNotes-2003-06
Backdoor.Sdbot.F	**F**	**Current Issue**
Backdoor.Serpa	N/A	CyberNotes-2003-03
Backdoor.Servsax	N/A	CyberNotes-2003-01

Trojan	Version	CyberNotes Issue #
Backdoor.SilverFTP	N/A	CyberNotes-2003-04
Backdoor.Sixca	N/A	CyberNotes-2003-01
Backdoor.Snowdoor	N/A	CyberNotes-2003-04
Backdoor.Socksbot	N/A	CyberNotes-2003-06
Backdoor.SubSari.15	15	CyberNotes-2003-05
Backdoor.SubSeven.2.15	2.15	CyberNotes-2003-05
Backdoor.SysXXX	N/A	CyberNotes-2003-06
Backdoor.Talex	N/A	CyberNotes-2003-02
Backdoor.Tankedoor	**N/A**	**Current Issue**
Backdoor.Turkojan	**N/A**	**Current Issue**
Backdoor.Udps.10	10	CyberNotes-2003-03
Backdoor.Unifida	N/A	CyberNotes-2003-05
Backdoor.Upfudoor	N/A	CyberNotes-2003-01
Backdoor.VagrNocker	N/A	CyberNotes-2003-01
Backdoor.Vmz	N/A	CyberNotes-2003-01
Backdoor.Xenozbot	N/A	CyberNotes-2003-01
Backdoor.Xeory	N/A	CyberNotes-2003-03
Backdoor.Zdemon	N/A	CyberNotes-2003-02
Backdoor.Zdown	N/A	CyberNotes-2003-05
Backdoor.Zix	N/A	CyberNotes-2003-02
Backdoor.Zvrop	N/A	CyberNotes-2003-03
Backdoor-AFC	N/A	CyberNotes-2003-05
Backdoor-AOK	N/A	CyberNotes-2003-01
BackDoor-AQL	N/A	CyberNotes-2003-05
BackDoor-AQT	N/A	CyberNotes-2003-05
BackDoor-ARR	ARR	CyberNotes-2003-06
Backdoor-ARU	ARU	CyberNotes-2003-06
BackDoor-ARX	ARX	CyberNotes-2003-06
BackDoor-ARY	ARY	CyberNotes-2003-06
BackDoor-ASD	**ASD**	**Current Issue**
BackDoor-ASL	**ASL**	**Current Issue**
BDS/AntiPC	N/A	CyberNotes-2003-02
BDS/Backstab	N/A	CyberNotes-2003-02
BDS/Ciadoor.10	**10**	**Current Issue**
BDS/Evolut	N/A	CyberNotes-2003-03
Daysun	N/A	CyberNotes-2003-06
DoS-iFrameNet	N/A	CyberNotes-2003-04
Downloader-BO.dr.b	N/A	CyberNotes-2003-02
Downloader-BS	N/A	CyberNotes-2003-02
Downloader-BW	N/A	CyberNotes-2003-05
Downloader-BW.b	BW.b	CyberNotes-2003-06
Downloader-BW.c	**BW.c**	**Current Issue**
Exploit-IISInjector	N/A	CyberNotes-2003-03
Hacktool.PWS.QQPass	N/A	CyberNotes-2003-06
ICQPager-J	N/A	CyberNotes-2003-05
IRC/Backdoor.e	E	CyberNotes-2003-01
IRC/Backdoor.f	f	CyberNotes-2003-02
IRC/Backdoor.g	g	CyberNotes-2003-03

Trojan	Version	CyberNotes Issue #
IRC/Flood.ap	N/A	CyberNotes-2003-05
IRC/Flood.bi	N/A	CyberNotes-2003-03
IRC/Flood.br	br	CyberNotes-2003-06
IRC-Emoz	N/A	CyberNotes-2003-03
IRC-OhShootBot	N/A	CyberNotes-2003-01
JS.Fortnight.B	B	CyberNotes-2003-06
JS.Seeker.J	J	CyberNotes-2003-01
JS/Seeker-C	C	CyberNotes-2003-04
JS_WEBLOG.A	A	CyberNotes-2003-05
KeyLog-Kerlib	N/A	CyberNotes-2003-05
Keylog-Razytimer	N/A	CyberNotes-2003-03
KeyLog-TweakPan	N/A	CyberNotes-2003-02
Linux/Exploit-SendMail	N/A	CyberNotes-2003-05
MultiDropper-FD	N/A	CyberNotes-2003-01
Pac	N/A	CyberNotes-2003-04
ProcKill-AE	N/A	CyberNotes-2003-05
ProcKill-AF	N/A	CyberNotes-2003-05
ProcKill-Z	N/A	CyberNotes-2003-03
PWS-Aileen	N/A	CyberNotes-2003-04
PWSteal.AlLight	N/A	CyberNotes-2003-01
PWSteal.Rimd	N/A	CyberNotes-2003-01
PWSteal.Senhas	N/A	CyberNotes-2003-03
PWS-Tenbot	N/A	CyberNotes-2003-01
PWS-WMPatch	**N/A**	**Current Issue**
QDel359	N/A	CyberNotes-2003-01
QDel373	1373	CyberNotes-2003-06
Qdel374	1374	CyberNotes-2003-06
Qdel375	1375	CyberNotes-2003-06
Qdel376	**1376**	**Current Issue**
Renamer.c	N/A	CyberNotes-2003-03
StartPage-G	G	CyberNotes-2003-06
Stoplete	N/A	CyberNotes-2003-06
Swizzor	**N/A**	**Current Issue**
Tellafriend.Trojan	N/A	CyberNotes-2003-04
Tr/Decept.21	**21**	**Current Issue**
Tr/DelWinbootdir	**N/A**	**Current Issue**
TR/Fake.YaHoMe.1	N/A	CyberNotes-2003-02
Tr/SpBit.A	A	CyberNotes-2003-04
TR/WinMx	N/A	CyberNotes-2003-02
Troj/Dloader-BO	N/A	CyberNotes-2003-02
Troj/Manifest-A	N/A	CyberNotes-2003-03
Troj/Qzap-248	N/A	CyberNotes-2003-01
Troj/SadHound-A	N/A	CyberNotes-2003-03
Troj/Slacker-A	A	CyberNotes-2003-05
Troj/Slanret-A	N/A	CyberNotes-2003-03
Troj/TKBot-A	A	CyberNotes-2003-04
TROJ_JBELLZ.A	A	CyberNotes-2003-02
TROJ_KILLBOOT.B	B	CyberNotes-2003-01
TROJ_RACKUM.A	A	CyberNotes-2003-05

Trojan	Version	CyberNotes Issue #
Trojan.Barjac	N/A	CyberNotes-2003-05
Trojan.Dasmin	N/A	CyberNotes-2003-01
Trojan.Dasmin.B	B	CyberNotes-2003-03
Trojan.Downloader.Aphe	N/A	CyberNotes-2003-06
Trojan.Downloader.Inor	N/A	CyberNotes-2003-02
Trojan.Grepage	N/A	CyberNotes-2003-05
Trojan.Idly	N/A	CyberNotes-2003-04
Trojan.Ivanet	N/A	CyberNotes-2003-02
Trojan.KKiller	N/A	CyberNotes-2003-01
Trojan.Poldo.B	B	CyberNotes-2003-02
Trojan.Poot	N/A	CyberNotes-2003-05
Trojan.ProteBoy	N/A	CyberNotes-2003-04
Trojan.PSW.Gip	N/A	CyberNotes-2003-06
Trojan.PSW.Platan.5.A	N/A	CyberNotes-2003-01
Trojan.PWS.QQPass.D	N/A	CyberNotes-2003-02
Trojan.Qforager	N/A	CyberNotes-2003-02
Trojan.Qforager.Dr	N/A	CyberNotes-2003-02
Trojan.Qwe	N/A	CyberNotes-2003-02
Trojan.Snag	N/A	CyberNotes-2003-02
Trojan.Unblockee	N/A	CyberNotes-2003-01
Uploader-D	D	CyberNotes-2003-06
Uploader-D.b	**D.b**	**Current Issue**
VBS.Kasnar	N/A	CyberNotes-2003-06
VBS.Moon.B	B	CyberNotes-2003-02
VBS.StartPage	N/A	CyberNotes-2003-02
VBS.Trojan.Lovcx	N/A	CyberNotes-2003-05
VBS/Fourcourse	N/A	CyberNotes-2003-06
W32.Benpao.Trojan	N/A	CyberNotes-2003-04
W32.CVIH.Trojan	N/A	CyberNotes-2003-06
W32.Socay.Worm	N/A	CyberNotes-2003-02
W32.Systentry.Trojan	N/A	CyberNotes-2003-03
W32.Xilon.Trojan	N/A	CyberNotes-2003-01
W32.Yinker.Trojan	N/A	CyberNotes-2003-04
W32/Igloo-15	N/A	CyberNotes-2003-04
Xin	N/A	CyberNotes-2003-03

AIM-Canbot: This is an AOL Instant Messenger (AIM) bot Trojan. It connects to an AIM chat session and accepts commands from remote malicious users. This Trojan executable uses an icon typically associated with AIM (a yellow, running, person). When run, the Trojan creates the file C:\SYSTEM.INI. A new AIM username is generated. The name starts with "aimb0t" followed by 8 random characters. This name, along with a hardcoded password, is written to the ini file, and is used by the bot to connect to a chat session. First, the Trojan creates a new account and then connects to a specified chat session, and sends the message: aimb0t reporting for duty.... This is to inform remote malicious users that the infected system is on-line. A registry run key is created to load the Trojan at startup:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\
Run "Startup" = %TrojanPath%

The bot provides the following functionality to a malicious user :

- Retrieve victim IP address, hostname, and configured DNS server
- Instruct bot to download, and execute files
- Alter signon and signoff sounds

BackDoor-ASD: This is a remote access Trojan. Different packed versions of the Trojan have been received. When run, the Trojan copies itself to Windows directory. The file name can be IEXPLORy.EXE or IEXPLORz.EXE depending on different packed version running. It creates the following registry key in order to run at Windows start up:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run "MSTestNB" = C:\WINDOWS\IEXPLORy.EXE (or IEXPLORz.EXE)

The Trojan searches current running processes and terminates processes with various names. It also overwrites the process file with the Trojan file itself. The Trojan deletes registry keys used by above processes, opens port 23433, and listens on the port. It sends notification message to various web sites via HTTP. The messages includes victim machine IP address, port opened, machine name, Trojan service name, and password information.

BackDoor-ASL (Alias: BackDoor-ASL.dll): This Trojan allows a remote malicious user to gain access to the compromised system for the purpose of stealing personal information. The Trojan does not function on Win9x/ME systems. When run, it copies itself to the WINDOWS (%WinDir%) directory as SVCHOST.EXE. The Trojan creates three files in the SYSTEM (%SysDir) directory:

- extapi.dll
- rascfg.dll
- sysmsg.dll

The SVCHOST.EXE file installs the remote access server components by injecting the EXTAPI.DLL and SYSMSG.DLL files into the Explorer.exe process. The EXTAPI.DLL file enables the following functions:

- remote shell operations
- retrieves Windows version, registered owner and organization name
- retrieves RAM and CPU speed
- send e-mail
- sniff network traffic

The SYSMSG.DLL file checks the title of each Windows displayed on the screen. It check the title of open Windows, looking for various titles. If these titles match, the date/time, Window name, Window buttons pressed, clicked menus, and typed keystrokes into that Window are captured and saved to a file named WORD.DLL in the SYSTEM (%SysDir%) directory. This WORD.DLL may be sent to the author via e-mail, using the Trojans internal SMTP engine. The RASCFG.DLL contains configuration information. The main Trojan executable is installed as a service:

- Name: System Important Message
- Path: C:\WINNT\svchost.exe -k ras

Backdoor.Delf.F: This is a Backdoor Trojan that gives a malicious user access to your computer. By default, it opens TCP ports 25226 and 45672. The existence of the file Svced.exe is an indication of a possible infection. Backdoor.Delf.F is a Delphi application. When Backdoor.Delf.F is executed, it copies itself as %System%\Svced.exe and adds the value, "Svced %System%\Svced.exe," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows. It also opens the TCP ports 25226 and 45672, allowing a malicious user to perform various actions.

Backdoor.Fluxay (Alias: BKDR_FLUXAY.A): This is a Backdoor Trojan Horse that uses pipes to allow an unauthorized command shell on an infected computer. It adds itself to the Service list as "PipeCmdSrv." When Backdoor.Fluxay is executed, it will add itself as a Service with the name, "PipeCmdSrv," and checks for the following named Pipes:

- \\.\pipe\PipeCmd_communicaton
- \\.\pipe\PipeCmd_stderr
- \\.\pipe\PipeCmd_stdin
- \\.\pipe\PipeCmd_stdout

The Trojan also redirects information from the communication pipe to the command, "cmd.exe /q /c."

Backdoor.FTP_Ana.C: This is a Trojan Horse that gives a malicious user access to your computer. Once the Trojan is installed, the malicious user is notified by ICQ pager. It listens on port 666, by default. When Backdoor.FTP_Ana.C runs, it moves itself to %Windir%\Nava32.exe and creates the value, “Nortan Anti Virus %Windir%\nava32.exe,” in the registry keys:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

It also creates the value, “StubPath %Windir%\nava32.exe ASC,” in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\Nortan Anti Virus

The Trojan modifies the Win.ini file by adding these lines in the [windows] section:

- run=%Windir%\nava32.exe
- load=%Windir%\nava32.exe

and modifies the [boot] section of the System.ini file as follows:

- shell=explorer.exe %Windir%\nava32.exe

It notifies the client side using ICQ pager. After Backdoor.FTP_Ana.C is installed, it waits for the commands from the remote client. The commands give a malicious user full access to the file system of the infected computer.

Backdoor.Graybird (Aliases: Backdoor.GrayBird, BackDoor-ARR): This is a Backdoor Trojan that gives a malicious user unauthorized access to your computer. The existence of the file Svch0st.exe is an indication of a possible infection. Backdoor.Graybird is a Delphi application. When Backdoor.Graybird runs, it copies itself as %System%\Svch0st.exe and creates the value, “svchost %System%\Svch0st.exe,” in the registry keys:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows. If the operating system is Windows NT/2000/XP, the Trojan also creates the value, “run %system%\svch0st.EXE,” in the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

If the operating system is Windows 95/98/ME, the Trojan adds the line, “run=C:\WINDOWS\SYSTEM\SVCH0ST.EXE,” to the [windows] section of the Win.ini file so that the Trojan runs when you start Windows. Then, it attempts to access the password cache stored on your computer. The cached passwords include the modem and dialup passwords, URL passwords, share passwords, and others. Next it intercepts keystrokes, which could allow Backdoor.Graybird to steal confidential information. Once Backdoor.Graybird is installed, it waits for the commands from the remote client.

Backdoor.OptixPro.12.b (Aliases: Backdoor.Optix.Pro.12, Backdoor:Win32/Optix.1_2): This is a Backdoor Trojan Horse that gives a malicious user full access to your computer. By default the Trojan opens port 2060 for listening. When Backdoor.OptixPro.12.b is executed, it copies itself as %System%\<name of original Trojan file> and inserts the file, %Windir%\Winampw.exe. Backdoor.OptixPro.12.b creates the value, “InternalSystray %system%\<name of original Trojan file>,” in the registry keys:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

so that the Trojan runs when you start Windows. Next it hooks the execution of the executable files by changing the (Default) value of the registry key:

- HKEY_CLASSES_ROOT\exefile\shell\open\command

to:, “winampw.exe "%1" %*.” This will cause Winampw.exe to be run every time you run any .exe file. This Trojan also modifies the Run= line of the Win.ini file to, “Run=%System%\<name of original Trojan file>,” so that the Trojan runs when you start Windows 95/98/ME. It modifies the Shell= line of the System.ini file to:

- Shell=<previous content> %system%\<name of original Trojan file>

so that the Trojan runs when you start Windows 95/98/ME. A listening port is opened on port 2060. (This is the default for this Trojan, but the malicious user can change it to any other port.)

Backdoor.OptixDDoS: This is a Backdoor Trojan that gives a malicious user access to your computer. The Trojan performs as an agent of a Distributed Denial of Service (DDoS) attack. It is a Delphi application and is packed with PECompact. When Backdoor.OptixDDoS is executed, it copies itself as \Windows\Java\apps\Winjava.exe. Your system information, such as IP, OS version, and RAS password, is send to the malicious user.

Backdoor.Rsbot (Aliases: Remote Script bot, BackDoor-ASE): This is a Backdoor Trojan Horse that gives a malicious user unauthorized access to your computer. Several variants have been found. All the variants are written in the Microsoft Visual C++ programming language. When Backdoor.Rsbot runs, it copies itself as %System%\Msapp.exe and adds the value, "WinApp32 msapp.exe," to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows. Next is modifies the shell= line in the System.ini file to, "Shell=Explorer.exe msapp.exe," so that the Trojan runs when you start Windows 95/98/ME. It also opens some randomly changed TCP and UDP ports, which allows a malicious user to remotely manipulate your computer and perform various actions.

Backdoor.Sdbot.F (Alias: Backdoor.SdBot.gen): This is a Backdoor Trojan that is a variant of Backdoor.Sdbot. It is a server component (bot) that a malicious user distributes over the IRC channels. This Trojan allows a malicious user to perform a wide variety of actions on your computer. It arrives as the file, RunDll16.exe. When Backdoor.Sdbot.F runs, it copies itself as the following files:

- %System%\RunDll16.exe
- %System%\Ms_32.exe
- %System%\Ms_bak.tmp.exe

Next it adds the value, "RDLL RunDll16.exe," to these registry keys:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

so that the Trojan runs when you start Windows. Backdoor.Sdbot.F contains its own IRC client, allowing it to connect to an IRC channel that was coded into the Trojan. Using the IRC channel, the Trojan listens for the commands from the malicious user. The malicious user accesses the Trojan by using a password-protected authorization.

Backdoor.Tankedoor (Aliases: Backdoor.Tankedoor.02, W32/Rbit.worm): This is a Backdoor Trojan that gives a malicious user access to your computer through an IRC channel. The existence of the file dllmem32.exe is an indication of a possible infection. Backdoor.Tankedoor is a Delphi application and is packed with ASPack. When Backdoor.Tankedoor is executed, it copies itself as %System%\Dllmem32.exe and adds the value, "DLL32"="%System%dllmem32.exe," to the registry keys:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runonce

On Windows NT/2000/XP computers, it modifies the value from: "Shell"="Explorer.exe" to: "Shell"="Explorer.exe %System%dllmem32.exe" in the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

Backdoor.Turkojan (Aliases: BackDoor.Turkojan.10, BackDoor-ARL, Backdoor.Antilam.g1): This is a Backdoor Trojan that gives a malicious user unauthorized access to a compromised computer. The strings used in the Trojan indicate that the Trojan generator may have produced it. Therefore, the malicious user, who is using the Trojan generator or patching the compiled executable, defines some characteristics of this Trojan. By default is opens port 31693. It is a Delphi application.

BDS/Ciadoor.10: Like other backdoors, BDS/Ciadoor.10 would potentially allow someone with malicious intent remote access to your computer. If executed, the backdoor adds a file with a random name to the \windows\ directory. So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run <random_name>=<random_name>.exe
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices <random_name>=<random_name>.exe

Downloader-BW.c (Alias: NED-09): This purpose of this Trojan is simply to download a file from the Internet and execute it. At the time of this writing, the Trojan downloaded another Trojan (PWS-WMPatch). When the downloader is run, it displays a fake error message. The Trojan connects to an angelcities.com user site to download a file named sysman32.exe to the WINDOWS SYSTEM (%SysDir%) directory. A registry run key is created to load this downloaded file at system startup:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ Run "SystemManager" = C:\WINDOWS\SYSTEM\sysman32.exe

The content of the downloaded file may vary, as the author can easily replace it on their website.

PWS-WMPatch (Alias: PWS-IN): This Trojan is written in MSVC++ and is compressed using PE-Pack. It may arrive in a spoofed e-mail suggesting it came from support@yahoo.com, pretending to be a software patch for PayPal/WebMoney software. Upon running the file, it displays no visible output. It is however visible in the windows task manager process list. The Trojan looks for cached passwords and tries to send an e-mail to a specific e-mail address in the Czech Republic by connecting to an specific IP address.

Qdel376: When the Trojan is executed, it will drop an empty SOS.bat into Program Files\ICQ. It will then copy all files from the Windows directory into the Windows SYSTEM directory. The files in the Windows directory will be overwritten with the following text message: “You are a fool! You are a fool! You are a fool! You are a fool! You are a fool! You are a fool!” The Trojan may reboot the system.

Tr/Decept.21: Like other Trojans, Tr/Decept.21 would potentially allow someone with malicious intent backdoor access to your computer. If executed, the backdoor adds a file with a random name to the \windows\ directory. So that it gets run each time a user restart their computer the following registry key gets added:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run <random_name>=<random_name>.exe

Both Variants, Tr/Decept.21.a and Tr/Decept.21.b are tools to pack two .EXE files into one .EXE file. If the .EXE file is run, it will install the virus infected .EXE file but show the regular .EXE file.

Tr/DelWinbootdir: Like other Trojans, Tr/DelWinbootdir would potentially allow someone with malicious intent backdoor access to your computer. If executed, the following file will be modified in the root directory, "msdos.sys.” It appears to be serial number cracker for Microsoft Frontpage. The MSFrontpage Key Generator shows a Serial Key and writes to the end of the msdos.sys file the following:

- [Paths]
- WinBootDir=0

Therefore, the next time the system is restarted Windows will not function correctly, stability will be lost. The file can be exchanged through the KaZaA file-sharing program.

Swizzor (Aliases: TrojanDownloader.Win32.Swizzor, TrojanDownloader.Win32.Swizzor.b) The TrojanDownloader.Win32.Swizzor.b is a small program that can come to a user's system when he or she is browsing the web. The program downloads and installs a LOP.COM-related plugin that acts as a spyware/adware and provides customized search capabilities.

Uploader-D.b (Alias: Karbsteal): This is a data-stealing Trojan that mails certain files to a specific e-mail address. The file is written in Borland Delphi, but is likely to be compressed with a runtime compressor such as UPX. The Trojan is a later variant of an existing threat detected as Uploader-D.a. When executed, the Trojan does not install itself in any manner on the victim machine. It builds a list of files matching the following wildcards on local and remote drives:

- *.DOC
- *.XLS
- SE*.DBX (targets sent messages folder for Outlook Express, "SENT ITEMS.DBX")

If matching files are found, the files are mailed to an e-mail address hardcoded within the Trojan. (Files named README*, WINWORD*, TEST* and WORD* are excluded from search.) The message is constructed using the Trojans own SMTP engine, and a legitimate French SMTP server is used for sending the mail. The mail is formatted as follows (the exact target e-mail address (@ifrance.com domain) has been masked to 'xxx'):

- From: IP address of victim machine (xxx@ifrance.com)
- To: xxx@ifrance.com
- Subject: "machine name" [IP address of victim machine]
- Attachments: base64 encoded files (with original filenames)